NORDMENN OG DIGITAL SIKKERHETSKULTUR 2019

NorSIS
Norsk senter for informasjonssikring

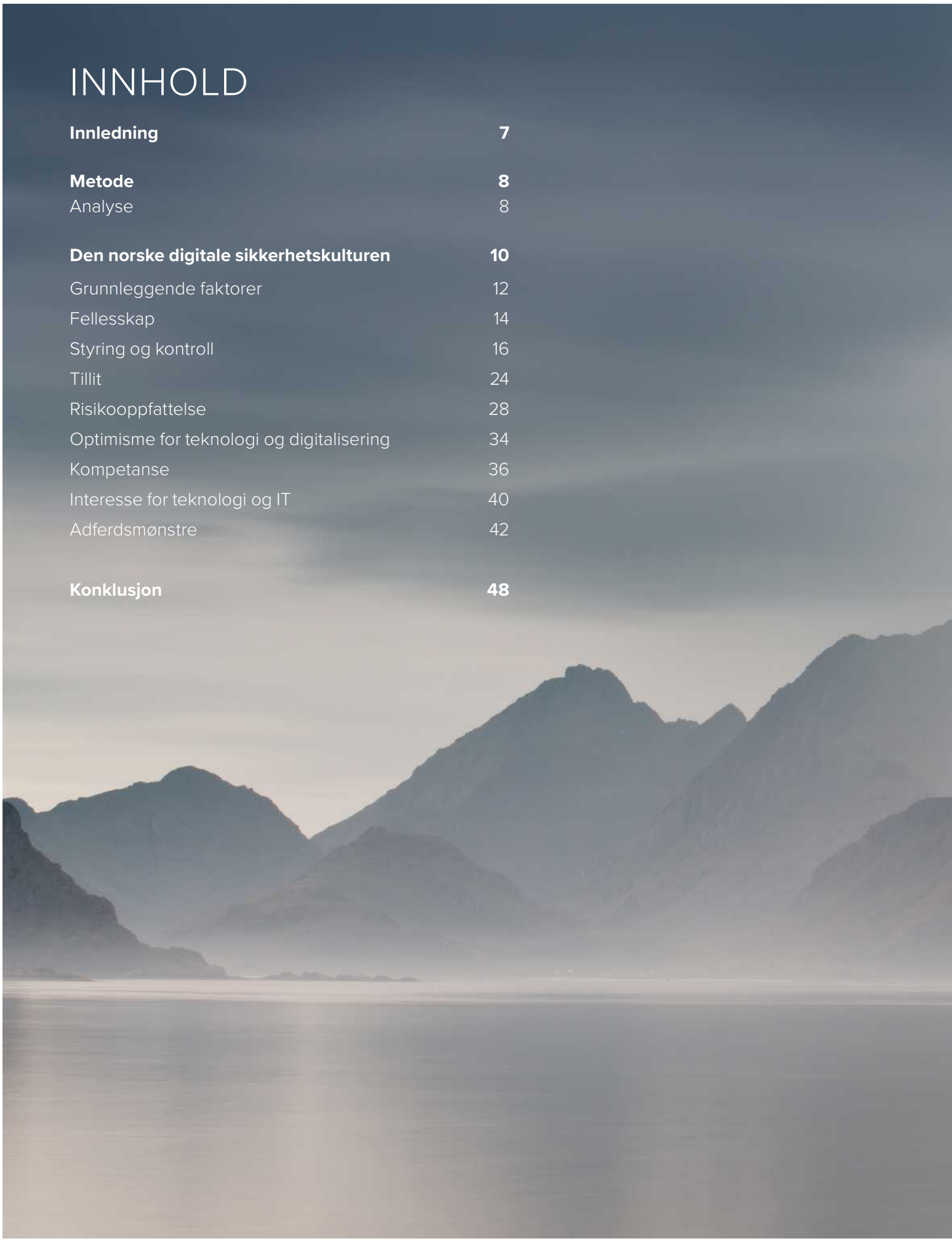
Ansvarlig: Peggy Sandbekken Heie
Forfattere: Bjarte Malmedal (metode og analyse) og Hanne Eggen Røislien (metode)
Design og informasjonsgrafikk: Sigve Ekseth Lundsaunet og Jørgen Westmo
Foto: Getty Images eller PxHere hvis ikke annet er oppgitt
ISBN: 978-82-93651-04-8

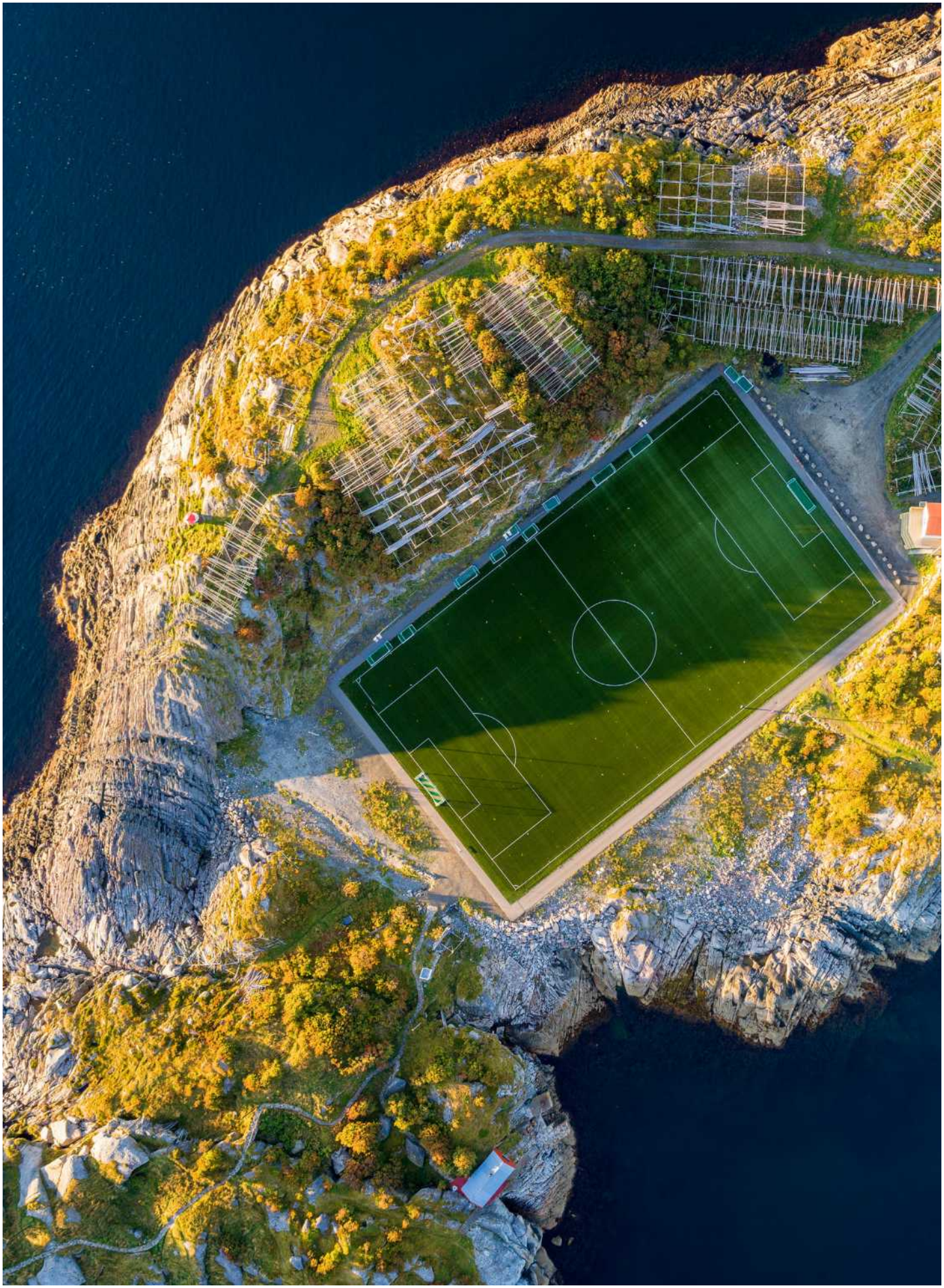
Undersøkelsen er gjennomført av analyseinstituttet YouGov. Det er i uke 11-12 gjennomført til sammen 1007 CAWI[1] -intervjuer i et landsrepresentativt utvalg 18+ år.

[1] *Computer Assisted Web Interview*

NORDMENN OG DIGITAL SIKKERHETSKULTUR

INNHOLD





INNLEDNING

DIGITAL SIKKERHETSKULTUR er våre felles verdier, holdninger, normer, kunnskaper og handlinger for å kunne ta del i et digitalisert samfunn på en trygg måte. Den digitale sikkerhetskulturen skal gjøre både den enkelte, og samfunnet i sin helhet, mer robuste mot digitale trusler. Dette bidrar til å bygge tillit til de digitale tjenestene. Denne tilliten er nødvendig for at vi skal kunne høste godene som digitaliseringen kan gi oss.

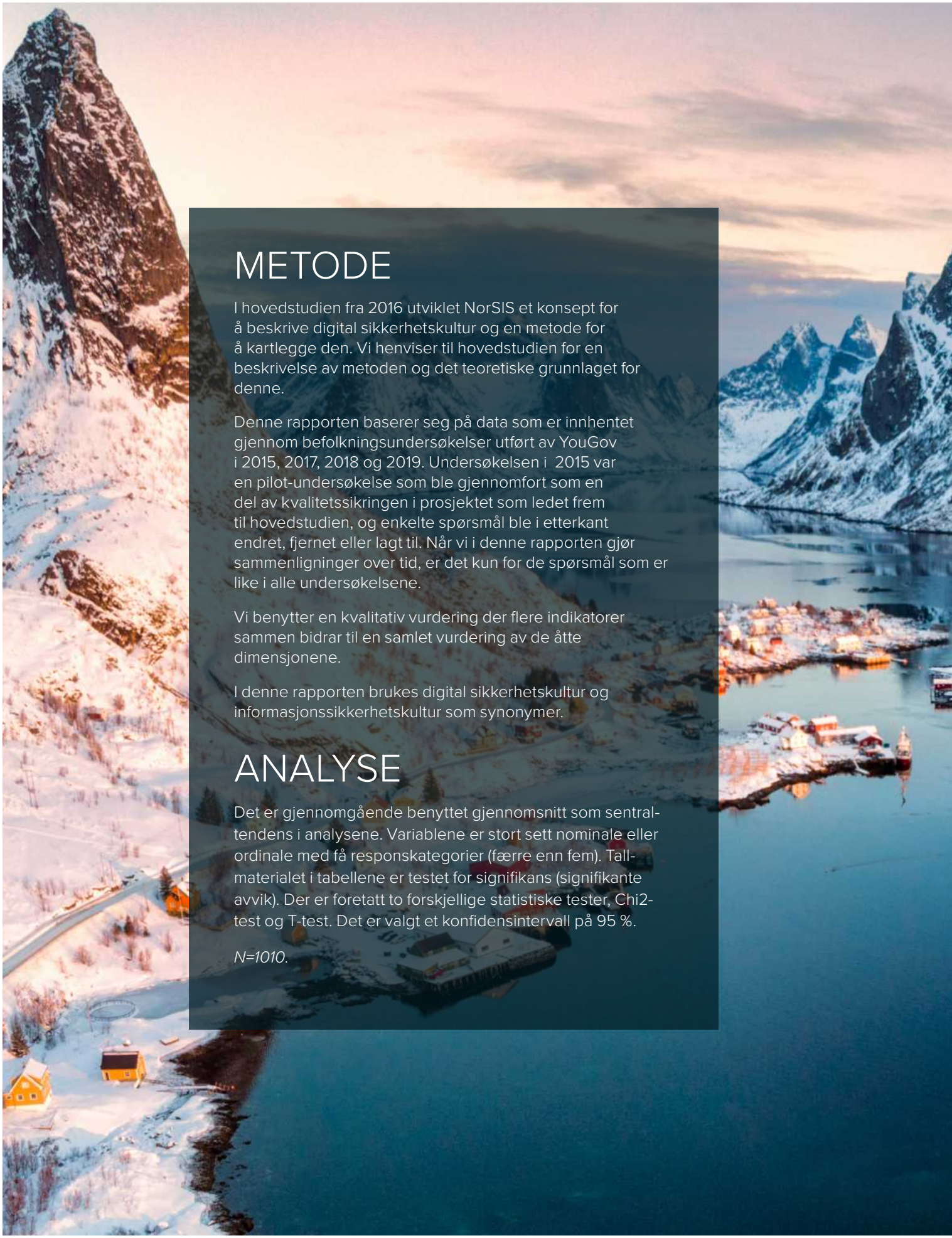
Siden NorSIS ga ut Nordmenn og digital sikkerhetskultur 2018, har det skjedd mye som vil kunne påvirke den nasjonale digitale sikkerhetskulturen i tiden fremover. Regjeringen har gitt ut strategiene *Nasjonal strategi for digital sikkerhet*, og *Nasjonal strategi for digital sikkerhetskompetanse*. Begge strategiene omfatter, i motsetning til tidligere strategier også den enkelte innbygger. I tillegg er digital sikkerhetskultur løftet frem som et område som skal prioriteres. Regjeringen har også lagt frem et forslag til ny lov om Etterretningstjenesten, som omfatter et forslag om såkalt «tilrettelagt innhenting» (tidligere omtalt som digitalt grenseforsvar). Dette forslaget har skapt sterke reaksjoner fra mange hold. I tillegg har vi siden forrige undersøkelse sett en jevn strøm av medieoppslag om trakassering, nettovergrep, datakriminalitet, bedragerier og andre uønskede hendelser på nett.

Å kartlegge den nasjonale digitale sikkerhetskulturen er et viktig verktøy for å kunne oppdage om disse tingene har noen effekt på våre holdninger og handlinger. Å endre holdninger og normer er selvsagt ikke gjort over natten. Men; når en ser at nasjonale tiltak ikke har ønsket effekt, eller når en ser at utviklingen går i feil retning, er det på tide å vurdere om man har valgt riktig strategi. I årets rapport ser vi at det fremdeles er under halvparten av de spurte som mener at politiet vil hjelpe dem dersom de blir utsatt for datakriminalitet. Samtidig som vi ser at det er en økende støtte til selvtekt på nett. Dette er to forhold som burde bekymre justissektoren. Vi mener derfor at det må evalueres om det gjøres nok, og nok av de riktige tingene, for å motvirke utviklingen.

NorSIS kartlegger den nasjonale digitale sikkerhetskulturen hvert år, vel vitende om at en ikke kan forvente å se dramatiske forskjeller fra år til år. Likevel lever vi i et samfunn hvor det digitale tar stadig større plass i vår felles bevissthet, og hvor store hendelser plutselig oppstår. Det kan være vanskelig å vite på forhånd hvordan større samfunnshendelser påvirker våre holdninger. Det er derfor viktig å samle kunnskap om dette for å kunne utvikle modeller for å forutsi hvordan nordmenn vil reagere i ulike situasjoner. Forslaget om lov for Etterretningstjenesten, og debatten som fulgte, har gjort lite inntrykk på folk flest. Selv når det ligger an til at deres aktivitet på nett skal underlegges et massivt overvåkingsregime. I tiden frem mot stortingsvalget vil vi trolig se at sosiale medier og andre digitale plattformer blir arenaer for påvirkningsoperasjoner. Å følge med på hvordan dette i så fall vil påvirke nordmenns holdninger til det digitale blir svært interessant for oss som arbeider for at alle skal være trygge på nett.

Vi håper denne rapporten er til nytte for alle som arbeider med digital sikkerhetskultur i Norge.

Rapporten er utarbeidet med støtte fra Justis- og beredskapsdepartementet.



METODE

I hovedstudien fra 2016 utviklet NorSIS et konsept for å beskrive digital sikkerhetskultur og en metode for å kartlegge den. Vi henviser til hovedstudien for en beskrivelse av metoden og det teoretiske grunnlaget for denne.

Denne rapporten baserer seg på data som er innhentet gjennom befolkningsundersøkelser utført av YouGov i 2015, 2017, 2018 og 2019. Undersøkelsen i 2015 var en pilot-undersøkelse som ble gjennomfort som en del av kvalitetssikringen i prosjektet som ledet frem til hovedstudien, og enkelte spørsmål ble i etterkant endret, fjernet eller lagt til. Når vi i denne rapporten gjør sammenligninger over tid, er det kun for de spørsmål som er like i alle undersøkelsene.

Vi benytter en kvalitativ vurdering der flere indikatorer sammen bidrar til en samlet vurdering av de åtte dimensjonene.

I denne rapporten brukes digital sikkerhetskultur og informasjonssikkerhetskultur som synonymer.

ANALYSE

Det er gjennomgående benyttet gjennomsnitt som sentral-tendens i analysene. Variablene er stort sett nominale eller ordinale med få responskategorier (færre enn fem). Tall-materialet i tabellene er testet for signifikans (signifikante avvik). Der er foretatt to forskjellige statistiske tester, Chi2-test og T-test. Det er valgt et konfidensintervall på 95 %.

N=1010.

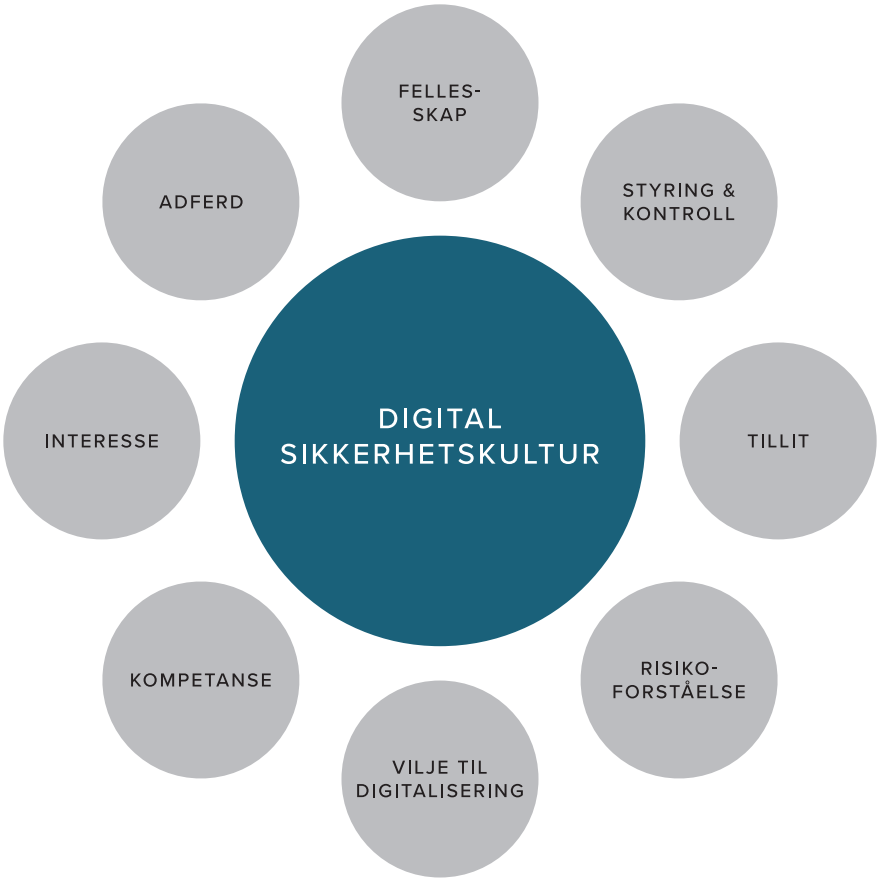
DEN NORSKE DIGITALE SIKKERHETS-KULTUREN

GRUNNLEGGENDE FAKTORER

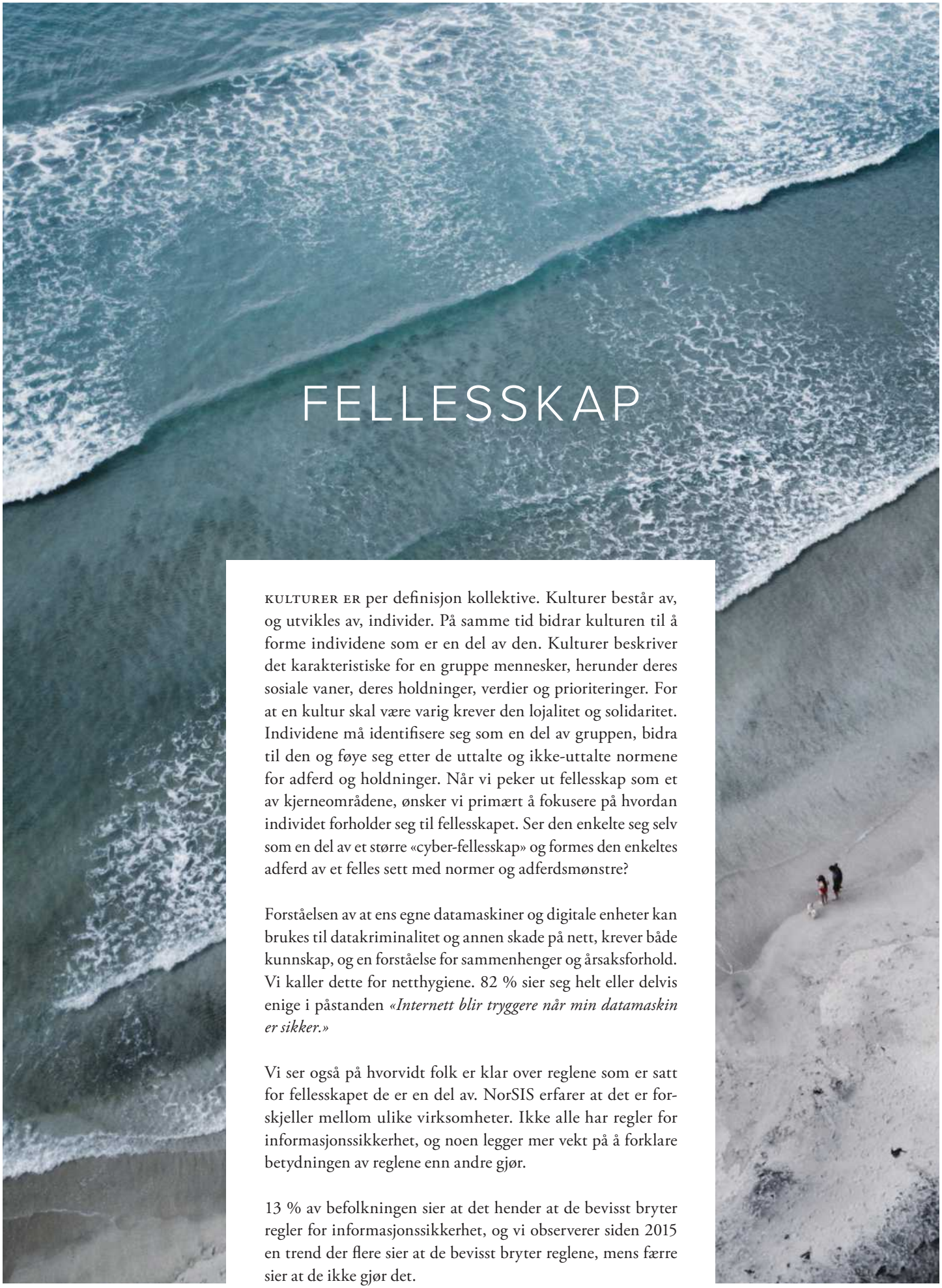
I HOVEDSTUDIEN I 2016 kartla vi kjerneelementene i den norske digital sikkerhetskulturen. Vi gikk bort fra antakelsen om at digital sikkerhetskultur kan beskrives utelukkende gjennom adferdsmønstre, men vurderte i stedet digital sikkerhetskultur gjennom et utvidet fokus på blant annet verdier, holdninger og følelser knyttet til ulike tema. Temaene spenner vidt, fra statlig styring og kontroll, til det individuelle synet på teknologikompetanse og risiko-oppfattelse.

ALLE KULTURER BALANSERER mellom det individuelle og det kollektive, mellom den enkeltes dømmekraft og oppfattelser av de kollektive normene og standardene. Ingen mennesker er fullstendige individualister eller fullstendig innlemmet i et større fellesskap. Studiet av digital sikkerhetskultur må derfor peke på de faktorene som beskriver en slik kultur i et helhetlig perspektiv, samtidig som de enkelte delene en digital sikkerhetskultur består av diskuteres og utfordres.

I DENNE STUDIEN har vi pekt ut åtte kjerneområder, eller dimensjoner, som vi mener beskriver digital sikkerhetskultur på en helhetlig og relevant måte. Det kan ikke utelukkes at det også finnes andre dimensjoner som kan være nyttig å betrakte, men for vårt formål anses disse utpekte kjerneområdene som tilstrekkelige.
Disse er:



Figur 1: *I det følgende beskriver vi de åtte kjerneområdene, og våre funn for befolkningens digitale sikkerhetskultur.*



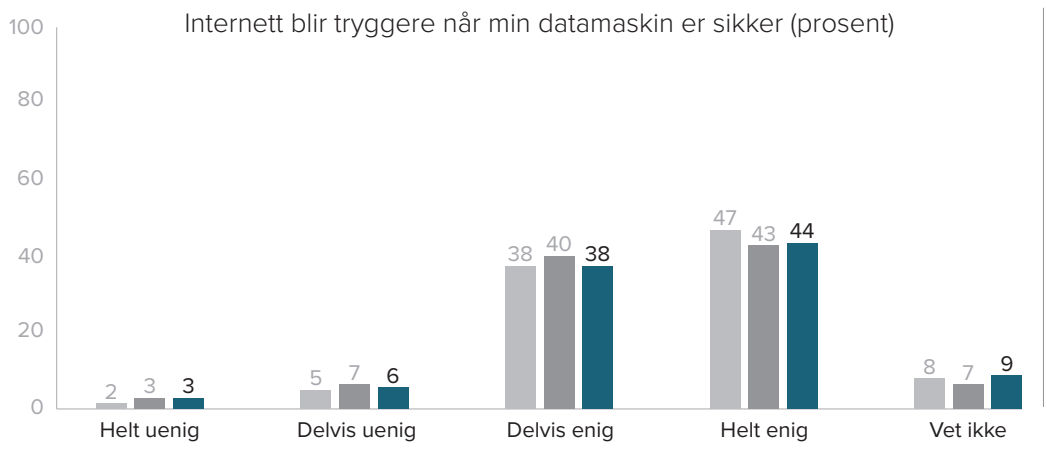
FELLESSKAP

KULTURER ER per definisjon kollektive. Kulturer består av, og utvikles av, individer. På samme tid bidrar kulturen til å forme individene som er en del av den. Kulturer beskriver det karakteristiske for en gruppe mennesker, herunder deres sosiale vaner, deres holdninger, verdier og prioriteringer. For at en kultur skal være varig krever den lojalitet og solidaritet. Individene må identifisere seg som en del av gruppen, bidra til den og føye seg etter de uttalte og ikke-uttalte normene for adferd og holdninger. Når vi peker ut fellesskap som et av kjerneområdene, ønsker vi primært å fokusere på hvordan individet forholder seg til fellesskapet. Ser den enkelte seg selv som en del av et større «cyber-fellesskap» og formes den enkeltes adferd av et felles sett med normer og adferdsmønstre?

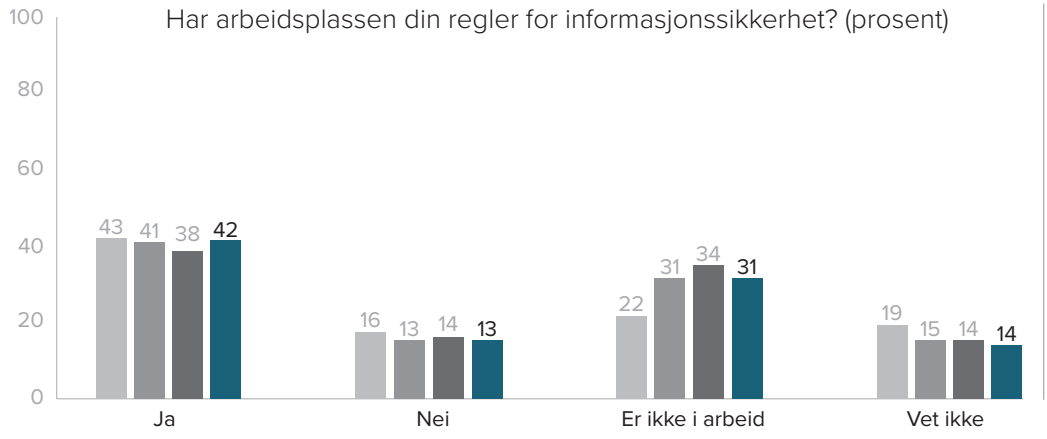
Forståelsen av at ens egne datamaskiner og digitale enheter kan brukes til datakriminalitet og annen skade på nett, krever både kunnskap, og en forståelse for sammenhenger og årsaksforhold. Vi kaller dette for netthygiene. 82 % sier seg helt eller delvis enige i påstanden *«Internett blir tryggere når min datamaskin er sikker.»*

Vi ser også på hvorvidt folk er klar over reglene som er satt for fellesskapet de er en del av. NorSIS erfarer at det er forskjeller mellom ulike virksomheter. Ikke alle har regler for informasjonssikkerhet, og noen legger mer vekt på å forklare betydningen av reglene enn andre gjør.

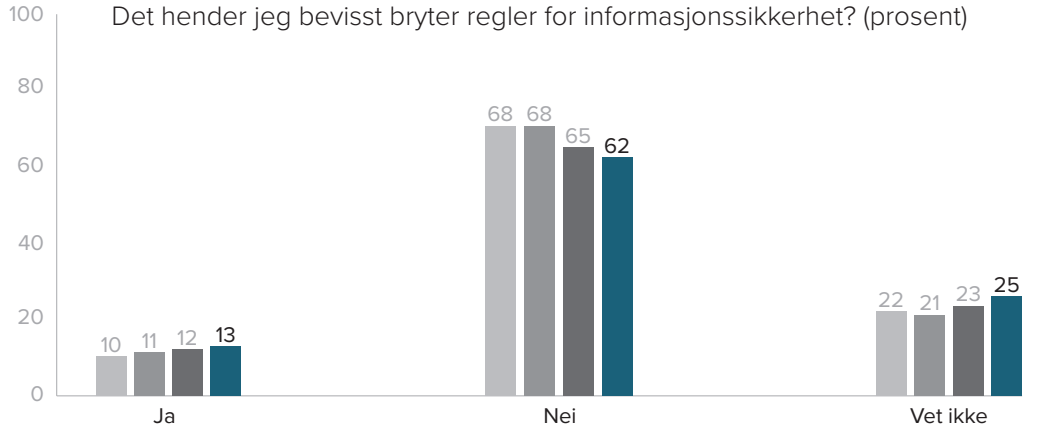
13 % av befolkningen sier at det hender at de bevisst bryter regler for informasjonssikkerhet, og vi observerer siden 2015 en trend der flere sier at de bevisst bryter reglene, mens færre sier at de ikke gjør det.



Figur 2:
Internett blir tryggere når datamaskinen min er sikker



Figur 3:
Har arbeidsplassen din regler for informasjons-sikkerhet?



Figur 4:
Det hender jeg bevisst bryter regler for informasjons-sikkerhet

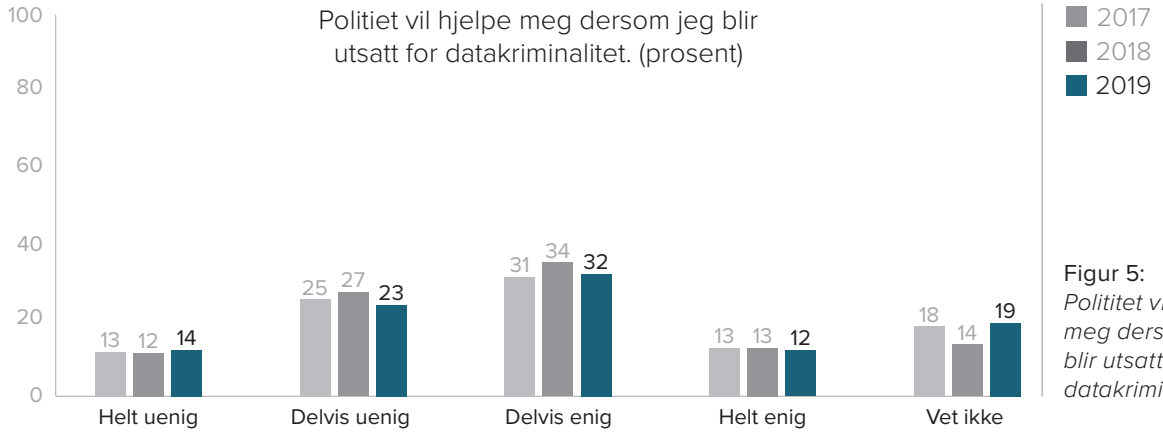

STYRING OG
KONTROLL

STYRING OG KONTROLL relaterer seg til fellesskap: Hvordan skal fellesskapet reguleres, og av hvem? I denne sammenhengen fokuserer vi på hvordan befolkningen ser på styring og kontroll i et digitalisert samfunn. Hvem trekker opp linjene for hva som er akseptabel bruk av IKT og digitale tjenester, hvor skal linjene trekkes opp og hvordan skal den enkelte rette seg etter disse? I befolkningen sier 44 % seg helt eller delvis enige i påstanden «*Politiet vil hjelpe meg dersom jeg blir utsatt for datakriminalitet*.» Dette er en svak nedgang fra 2018. Det er samtidig 37 % som sier seg helt eller delvis uenige i denne påstanden. Styring og kontroll vil i noen tilfeller dreie seg om inngripende metoder og maktbruk overfor den enkelte. Befolkningens tillit til politiet er derfor av stor interesse. Manglende tillit til politiet kan også trolig føre til at flere mener at privatpersoner og aktivister skal ha en rolle i kriminalitetsbekjempelse.

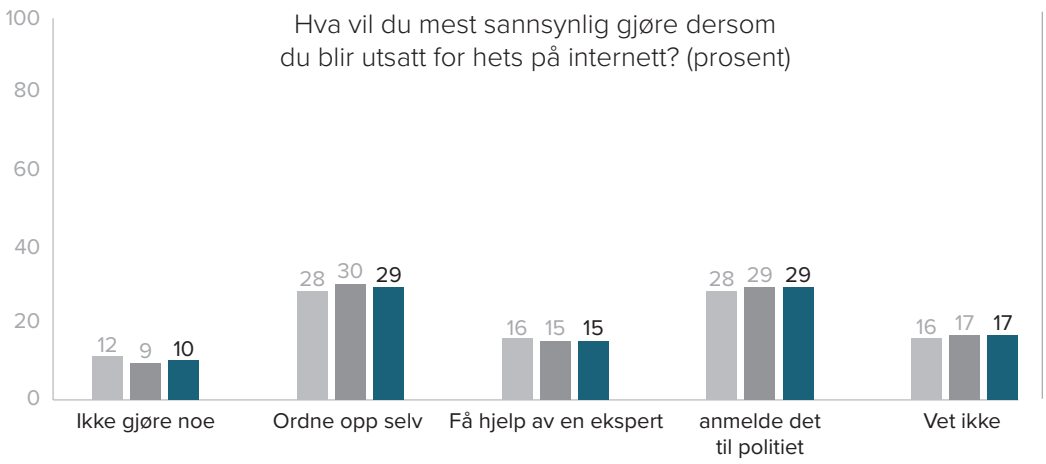
NorSIS mener at det er nedslående at politiet ikke har klart å bygge opp en større tillit i befolkningen til at de vil kunne hjelpe dem som blir utsatt for datakriminalitet. Når stadig mer av vår hverdag blir digitalisert, er tryggheten om at en vil få hjelp dersom en blir utsatt for datakriminalitet helt grunnleggende. Selv om politiet gjør mye som er bra, viser denne undersøkelsen at det er behov for en enda større satsing på dette.

I tillegg til å se på hvorvidt befolkningen tror at politiet vil kunne hjelpe dem dersom de blir utsatt for datakriminalitet, ser vi på hvorvidt den enkelte vil oppsøke hjelp fra de som er satt til å håndheve kriminalitetsbekjempelse på nett. Hets, nettsvindel og ID-tyverier rammer mange nordmenn hvert år. Dette er ofte forhold som kan være ulovlige, og som derfor bør etterforskes av politiet. 29 % av befolkningen svarer at de vil kontakte politiet dersom de blir utsatt for hets på internett. For nettsvindel og ID-tyverier, svarer henholdsvis 63 % og 72 % det samme.

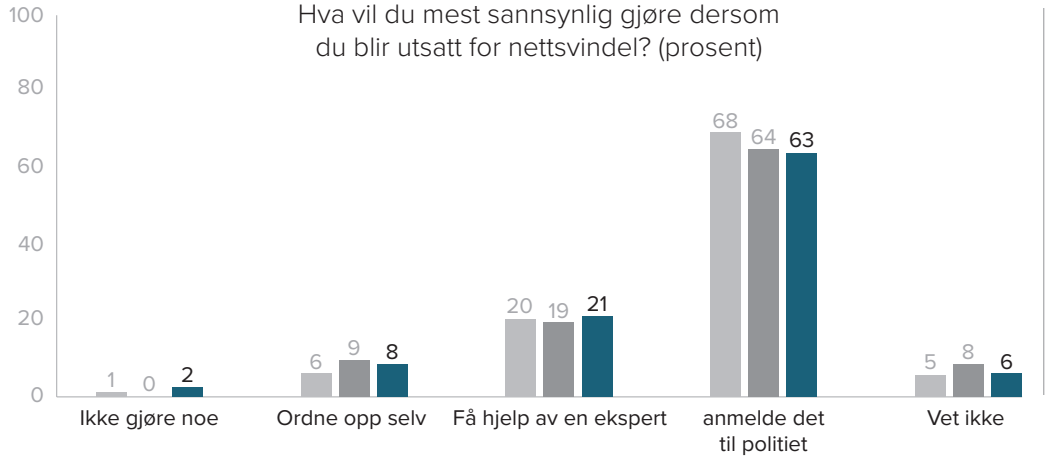
En mulig forklaring på at så mange færre sier de vil ta kontakt med politiet dersom de opplever hets kan være at slike hendelser oppleves som mindre alvorlige enn henholdsvis nettsvindel og ID-tyverier. En annen forklaring kan være at det oppleves som at det ikke vil nytte fordi politiet i liten grad prioriterer denne type hendelser.



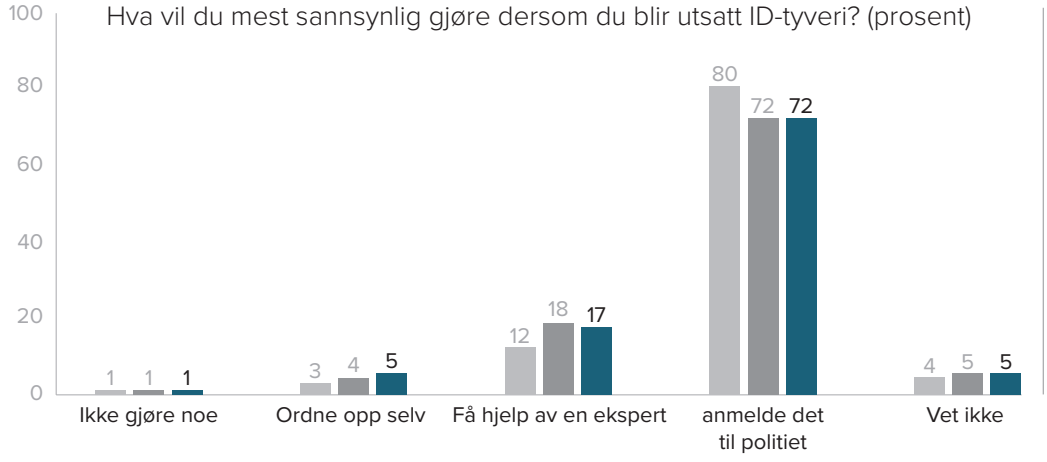
Figur 5:
Polititet vil hjelpe meg dersom jeg blir utsatt for datakriminalitet



Figur 6:
Hva vil du mest sannsynlig gjøre dersom du blir utsatt for hets på internett?



Figur 7:
Hva vil du mest sannsynlig gjøre dersom du blir utsatt for nettsvindel?



Figur 8:
Hva vil du mest sannsynlig gjøre dersom du blir utsatt for ID-tyveri?

I synet på om hvorvidt fellesskapet skal kunne gjennomføre overvåking og kontroll er flertallet enige i påstanden «*Det er greit at min aktivitet på internett blir overvåket dersom det fører til at jeg blir tryggere på nett*». På tross av debatten om lovforslaget for Etterretningstjenesten hvor Etterretningstjenesten gis mulighet til såkalt «tilrettelagt innhenting» (tidligere omtalt som digitalt grenseforsvar), er det ikke noen store endringer i befolkningens holdning til dette spørsmålet. Tidligere har politiets ønsker om økt datalagring og teknologiselskapenes innsamling av data om den enkelte vært oppe til diskusjon. Ettersom flere slike debatter oppstår, vil en kunne se for seg at det samlet sett kunne føre til en holdningsendring omkring dette spørsmålet.

Et spørsmål en kan stille seg er hvorvidt befolkningen har fått med seg at lovforslaget har blitt lagt frem, og om de har fulgt med på den påfølgende ordvekslingen om forslaget i nyhetsbildet og sosiale medier. Vi har derfor spurt befolkningen om de har satt seg inn i hovedtrekkene i lovforslaget.

Det er kun en av fem som sier at de har satt seg inn i hovedtrekkene i lovforslaget. Dette kan virke lavt. Samtidig skal en i denne sammenhengen huske at selve lovforslaget er svært krevende å sette seg inn i. Både fordi det er svært omfattende og fordi det har et språk som for mange er krevende å forstå. I tillegg inneholder det heller ikke mange av de detaljene som ville gitt noen av de svarene som mange er opptatt av. Den enkelte innbygger kan ved å lese lovforslaget egentlig ikke vite om akkurat deres aktivitet på nett ville blitt overvåket, og i så fall hvilke deler av deres aktivitet som ville blitt det.

Det er verdt å merke seg at en fjerdedel av de spurte ikke har hørt om lovforslaget. Det mener NorSIS er uheldig ettersom dette tross alt er et lovforslag som, dersom det blir besluttet innført, vil berøre alle personer i Norge.

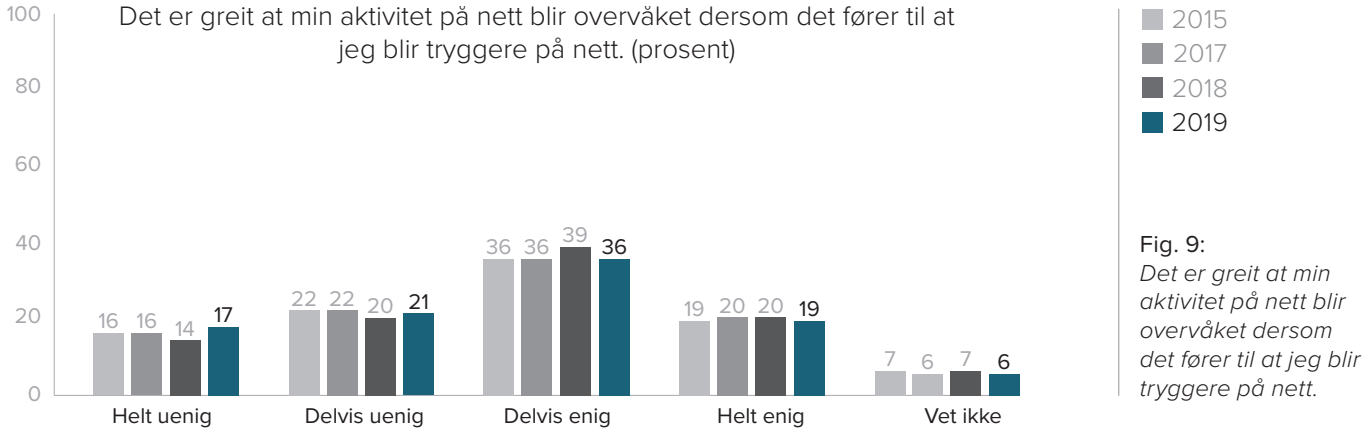


Fig. 9:
Det er greit at min aktivitet på nett blir overvåket dersom det fører til at jeg blir tryggere på nett.

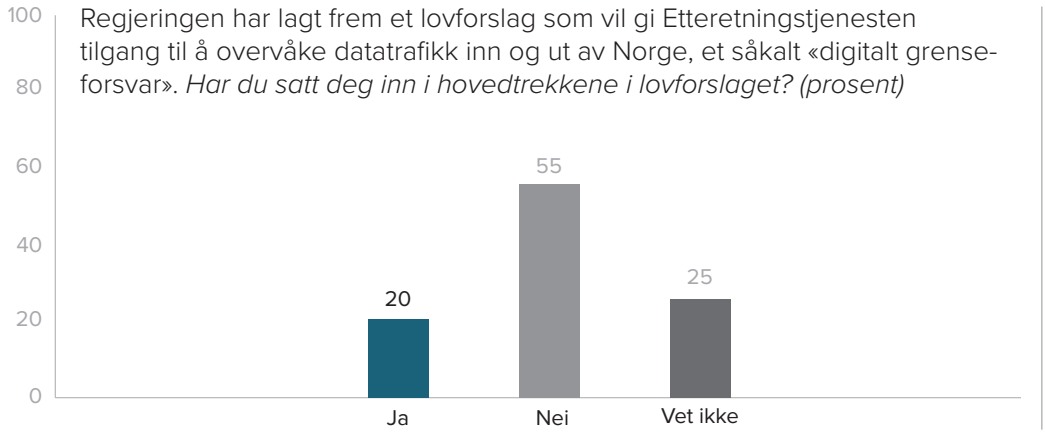


Fig. 10:
Kjennskap til lov om Etteretnings-tjenesten

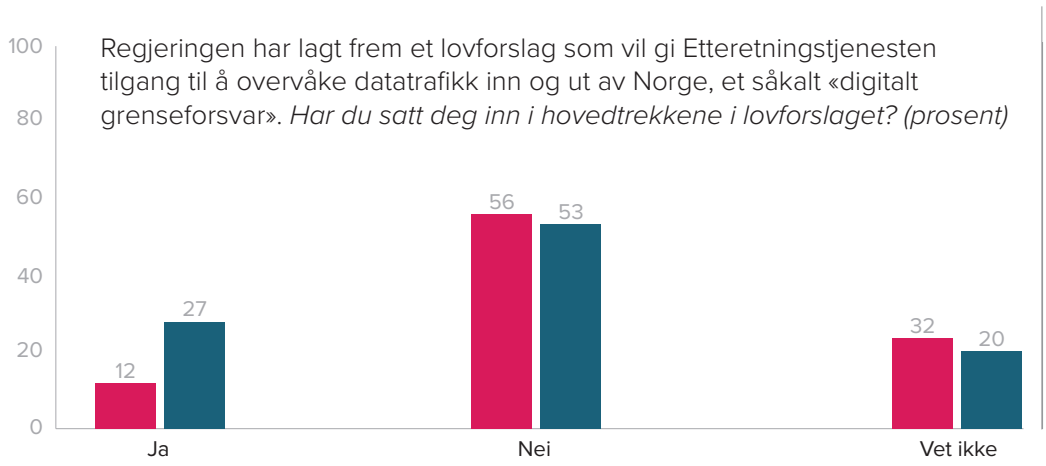


Fig. 11:
Kjennskap til lov om Etteretnings-tjenesten, forskjell mellom kvinner og menn

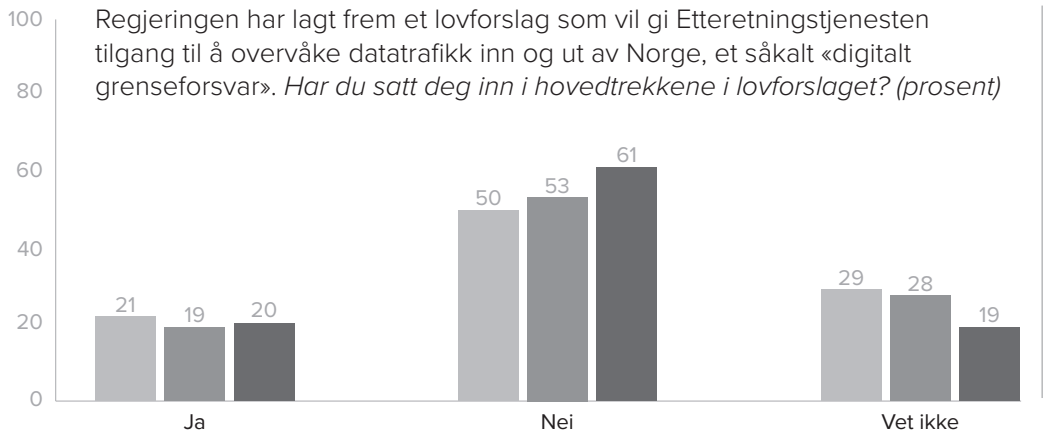
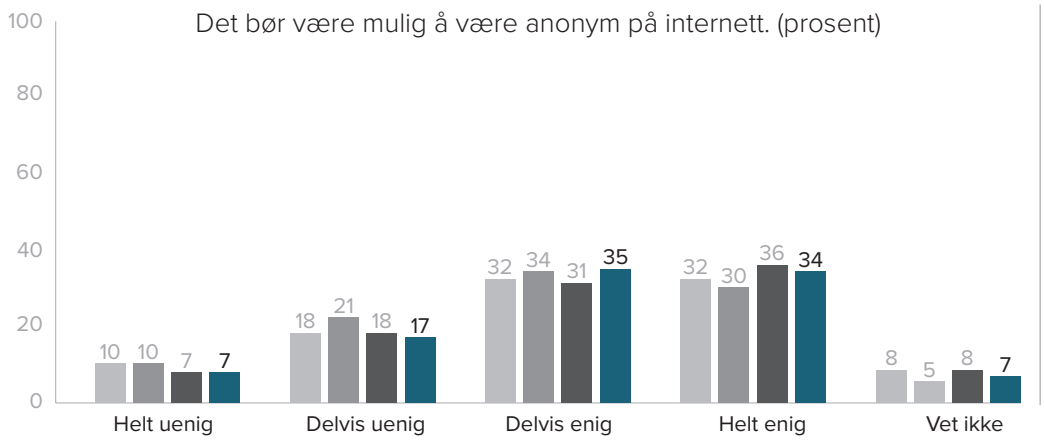


Fig. 12:
Kjennskap til lov om Etteretnings-tjenesten, forskjell mellom alders-grupper.



Figur 13:
Det bør være mulig å være anonym på internett

Spørsmålet om anonymitet på nett er beslektet fordi anonymitet kan være en måte å unndra seg kontroll. 69 % av de spurte sier seg helt eller delvis enige i at «*Det bør være mulig å være anonym på internett*». Vi observerer heller ikke her store endringer i perioden 2015-2019.

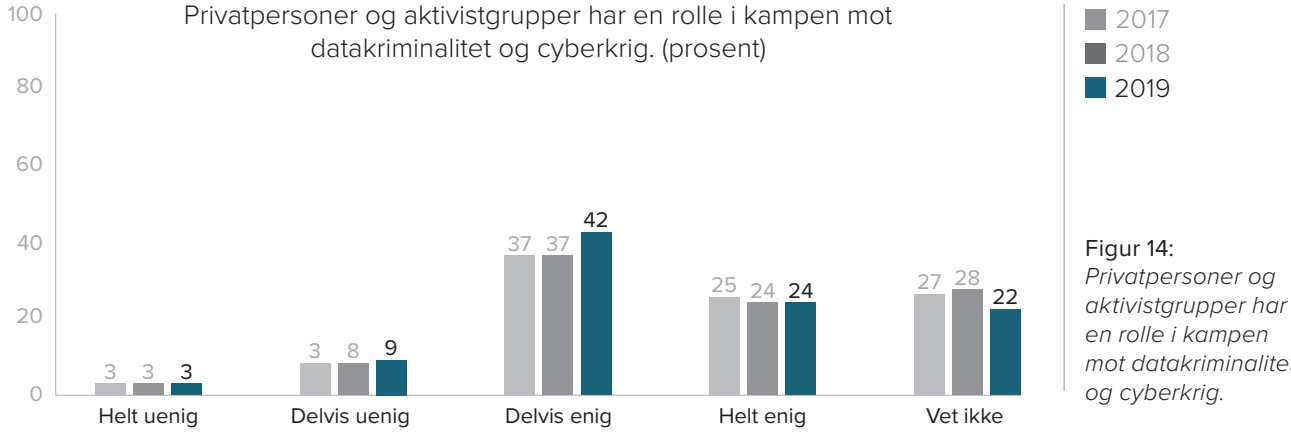
En annen side ved dette er om den enkelte innbygger aksepterer samfunnets normer for hvem som lager reglene, og hvem som håndhever dem. Den enkeltes rettssikkerhet baserer seg blant annet på at maktutøvelse er styrt av rettsregler.

Når det gjelder datakriminalitet registrerer vi at enkelte hevder at politiet verken har kompetanse eller ressurser til å etterforske slike saker. Det gjør at det er nødvendig at IKT-kyndige privatpersoner og grupperinger tar tak i problemet. En holdning om at privatpersoner har en rolle i kampen mot datakriminalitet bryter mot prinsippene for rettshåndhevelse som fellesskapet har besluttet. Årets undersøkelse viser at hele 66 % av de spurte er helt eller delvis enig i påstanden «*Privatpersoner og aktivistgrupper har en rolle i kampen mot datakriminalitet og cyber-krig.*»

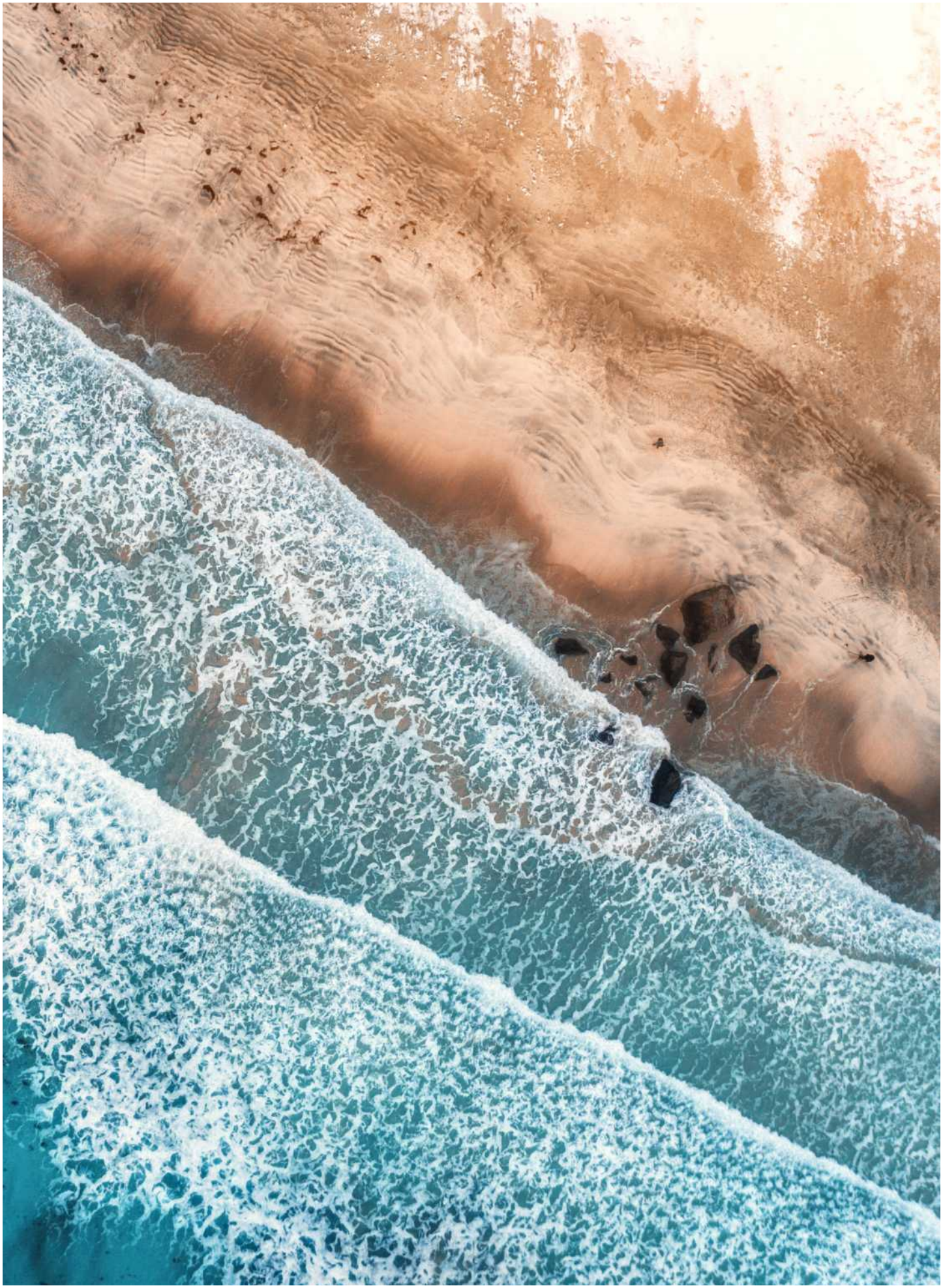
Dette mener vi i NorSIS er problematisk. Vi er først og fremst skeptiske til at norske IT-eksperter på fritiden deltar, anonymt, i internasjonale nettverk som tar loven i egne hender for å kjempe mot datakriminalitet. Vi vet lite om hvordan dette utføres, og de fleste som opererer i disse nettverkene er anonyme. Vi vet heller ikke om slike nettverk i verste fall kan bli infiltrert og brukes til sabotasje og spionasje mot Norge. Det er et viktig prinsipp at denne type etterforskning skal utføres av politiet. Rettssikkerheten til hver enkelt nordmann er tuftet på at maktutøvelse, som dette synes å være, styres av rettsregler. Det er lite trolig at det er tilfellet her, ettersom dette ofte er snakk om anonyme nettverk som opererer uten tilsyn og uten politiets kunnskap om å drive etterforskning.

Dette handler om en grenseoppgang mellom privatpersoner, virksomheter og politimyndighetene. Når det gjelder håndtering av datakriminalitet har ikke dette helt funnet sin form. Manglende kunnskap og prioriteringer hos politiet har skapt en gråsone som andre har søkt å fylle. Problemet oppstår når disse ikke har kunnskap om, eller forholder seg til regler og metoder som en etterforskning skal følge i en rettsstat.

I tillegg til at vi er skeptiske til at IT- eksperter driver selvstendig etterforskning på nett, mener NorSIS mener det er problematisk at så mange støtter at dette foregår. Det kan bidra til å legitimere en selvtektskultur på nett. Denne type grupper kan også inspirere andre, uten det samme etiske kompasset, til å ta loven i egne hender. At privatpersoner og grupperinger etterforsker andre uten å være underlagt de samme kontrollmekanismene som politiet er svært uheldig. Vi mener derfor myndighetene bør se nærmere på dette.



Figur 14:
Privatpersoner og aktivistgrupper har en rolle i kampen mot datakriminalitet og cyberkrig.




TILLIT

ET DEMOKRATI FORUTSETTER en viss tillit mellom innbyggerne, mellom innbyggerne og myndighetene, mellom myndighetsorganer, mellom bedrifter, mellom ansatte og arbeidsgivere og så videre. Når stadig mer av vår nasjonale økonomiske vekst og velferd er knyttet til digitalisering av samfunnet, blir tillit på dette området stadig viktigere.

For at myndighetene skal kunne styre effektivt, er de avhengig av innbyggernes tillit. I dette ligger det også at myndighetene må kunne styre selv om noen av innbyggerne er uenige i politikken. De må også ha befolkningens tillit til å innføre tiltak som er fremmede eller nye for innbyggerne.

Som en konsekvens av dette er digitaliseringen både avhengig av, og sårbar for, tillit. Digitalisering er en ønsket utvikling for de fleste nasjoner, og gitt den teknologiske utviklingen som omgir oss er det nærmest uunngåelig. For innbyggerne kan det imidlertid oppstå visse dilemma. Folk blir ikke bare oppfordret til å ta i bruk teknologi, de blir i noen tilfeller tvunget til det. Å være bankkunde i dag betyr at du må forholde deg til nettbank. Prisene for bank-transaksjoner i tradisjonelle banker øker sterkt. I tillegg er tilgjengeligheten til bankfilialene sterkt redusert fordi stadig flere av dem legges ned.

Kommunikasjonen mellom den enkelte og det offentlige skal primært foregå digitalt. Dersom den enkelte ikke føyer seg etter denne utviklingen, risikerer de både å glipp av de positive gevinstene ved digitaliseringen, og de får i noen tilfeller store ulemper ved å ikke rette seg etter det samfunnet har lagt opp til.

Når det digitaliserte samfunnet krever at den enkelte skal ta i bruk digitale tjenester og verktøy, forutsettes det at innbyggerne har tilstrekkelig tillit til disse. Først og fremst må tjenestene være sikre. Innbyggerne vil kanskje ikke tolerere mange sikkerhetsbrudd før de vil unngå å bruke de digitale tjenestene, og i verste fall miste tilliten til de som leverer dem.

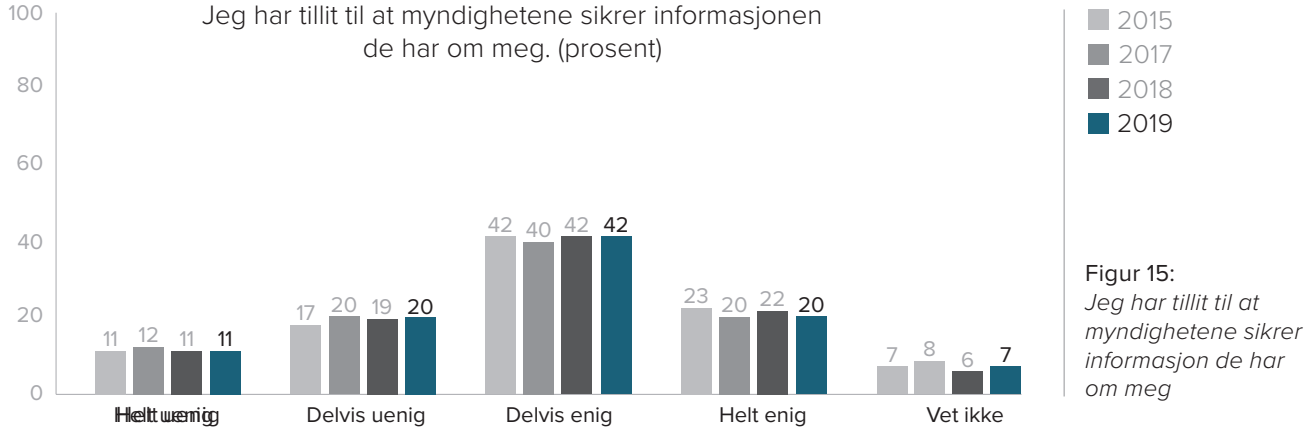
Også andre former for tillit spiller inn. Når forbrukere handler varer og tjenester på nett, overlates bank- og kredittkort, og annen personlig informasjon, til andre parter. Å velge å gjøre dette, indikerer en tillit til at disse partene vil beskytte denne informasjon mot misbruk. Det er likevel en balansegang, siden de fleste samtidig vet at Google, Facebook, Apple og andre bruker denne informasjonen til å profilere sine kunder. Profilene selges og brukes så til målrettet markedsføring. Som forbruker stilles en derfor ovenfor et dilemma: *Må det å kjøpe en bok på Amazon bety at jeg må åpne for at Amazon og deres partnere skal drive målrettet markedsføring ovenfor meg?*

Målrettet markedsføring er på et vis medaljens bakside, når det kommer til digitalisering og tillit. Mange anser målrettet markedsføring som et tillitsbrudd, ettersom leverandørene av digitale tjenester bruker informasjon om den enkelte til sin egen vinning. Dersom dette leder til redusert tillit kan det potensielt skade digitaliseringen av samfunnet.

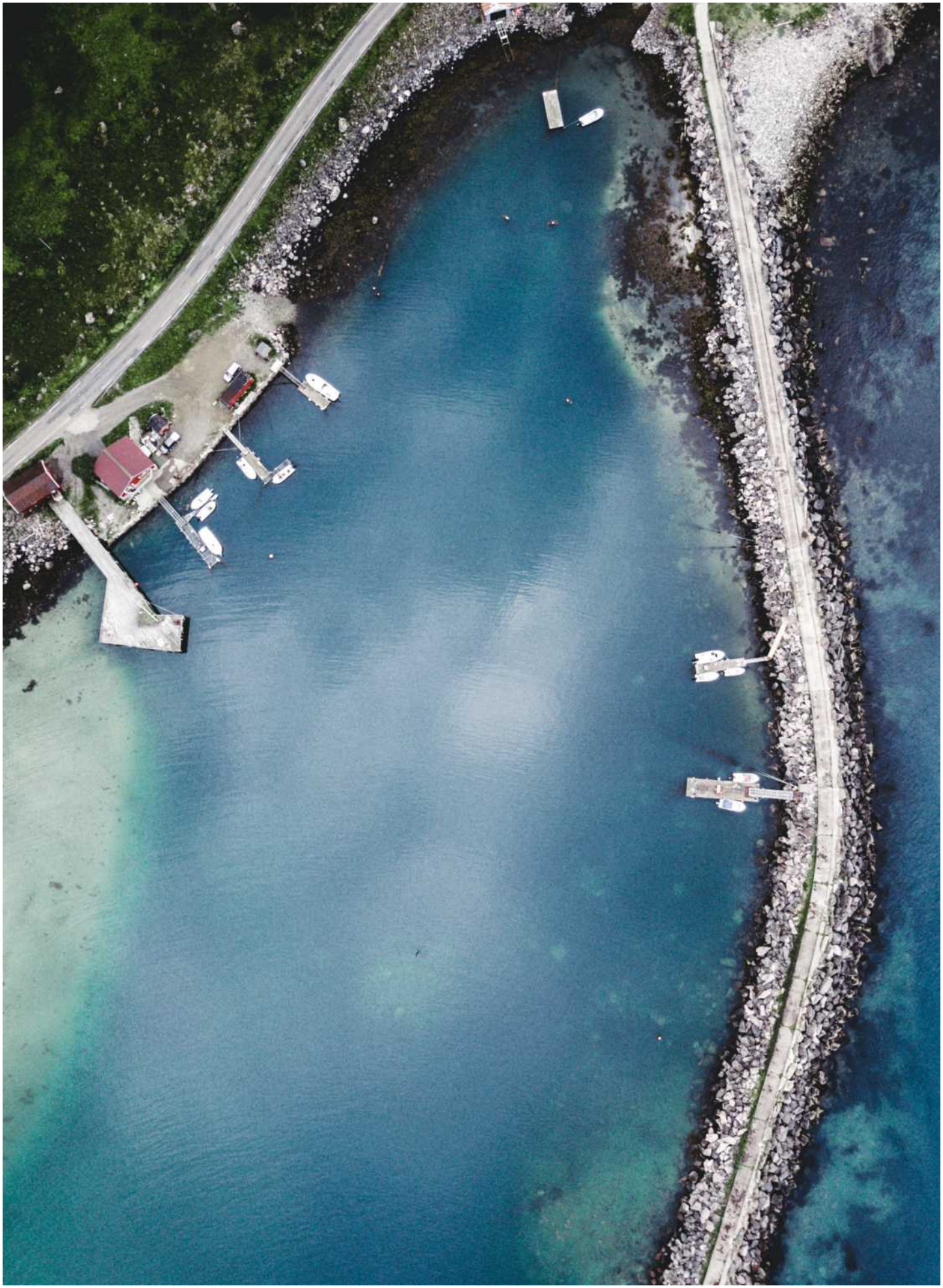
Tillit i denne sammenheng kan være gjensidig tillit mellom enkeltpersoner, virksomheter og myndigheter. Tillit i et digitalt samfunn er blant annet knyttet til transaksjoner og handel mellom mennesker som kanskje aldri møtes. Forbrukeren gir fra seg penger fordi vedkommende har tillit til at den andre parten leverer det som er avtalt. Innbyggerne gir fra seg informasjon til nett-selskaper fordi de har tillit til at selskapene ikke bruker informasjonen til å skade dem.

Vi har til nå sett på befolkningens syn på overvåking, anonymitet og kontroll. Tilliten til at politiet kan eller skal hjelpe med generell nettkriminalitet er relativt lav (44 %), men det er også verdt å legge merke til at langt de fleste sier at de vil be politiet om hjelp dersom de blir utsatt for nettsvindel eller ID-tyveri.

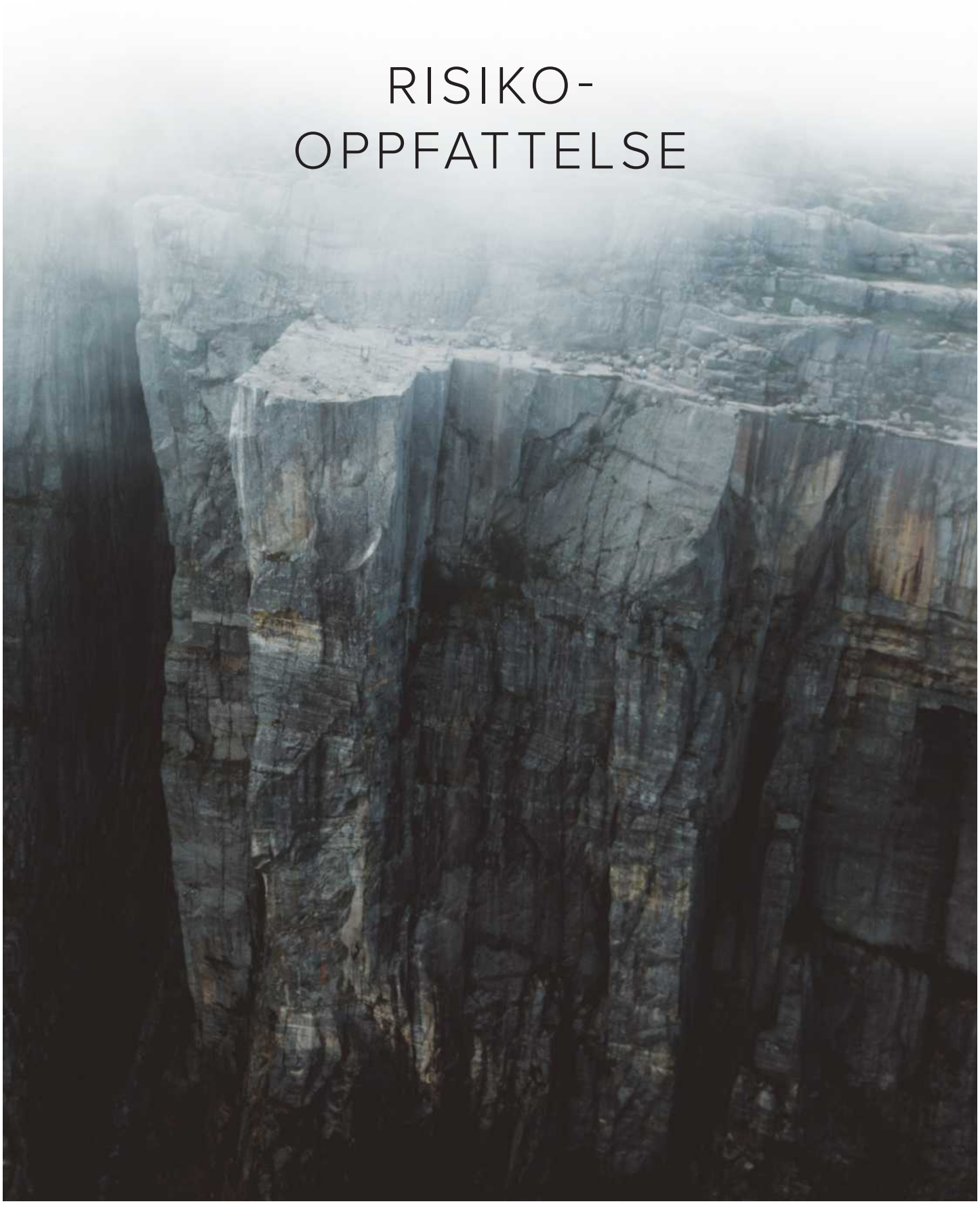
Til påstanden «*Jeg har tillit til at myndighetene sikrer informasjonen de har registrert om meg*», svarer 64 % at de er helt eller delvis enige i dette, mens 30 % svarer at de er helt eller delvis uenige. At en tredjedel av befolkningen ikke har tillit til at myndighetene sikrer informasjonen deres, er etter vårt syn svært alvorlig. Det er fordi dette kan motvirke digitaliseringen i samfunnet ved at folk ikke ønsker å ta i bruk de digitale tjenestene som myndighetene legger opp til.



Figur 15:
Jeg har tillit til at myndighetene sikrer informasjon de har om meg



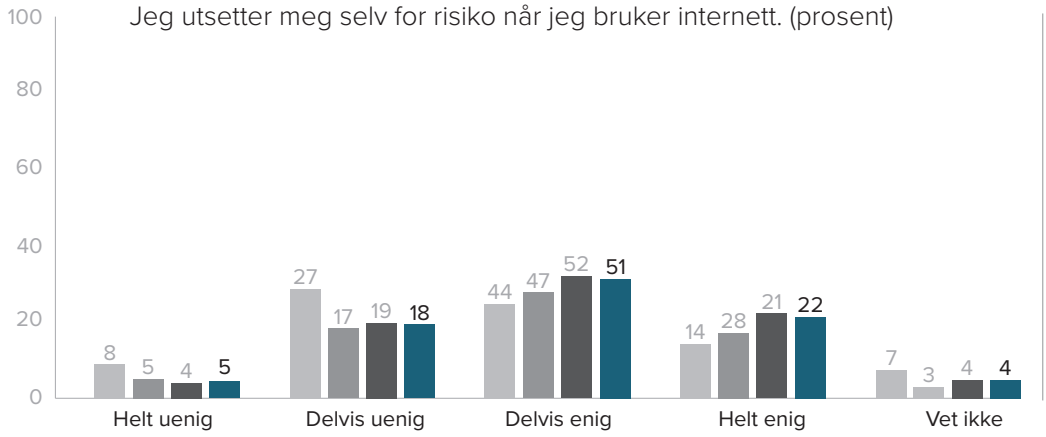
RISIKO-
OPPFATTELSE



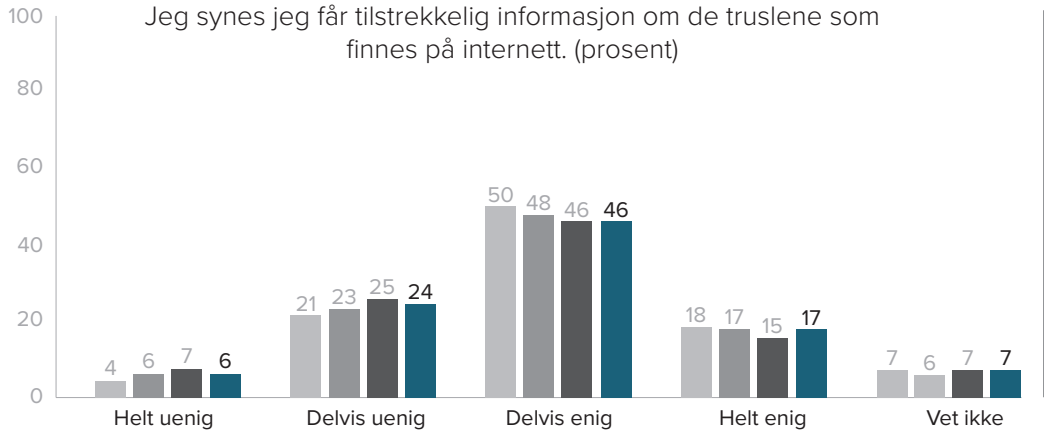
KOMPETANSE, LÆRING OG RISIKO-OPPFATTELSE er knyttet til hverandre. Hvordan den enkelte oppfatter risiko er subjektivt, men er likevel en viktig faktor som påvirker hvordan den enkelte tenker og handler når det kommer til digitale trusler. Det er en faktor som kan være vanskelig å tallfeste, beregne og forutse. Likevel vet vi at risiko-oppfattelsen vil bli påvirket av sikkerhetshendelser, hva den enkelte tror han eller hun vet om digitale trusler, erfaringer på nett og så videre.

73 % av befolkningen er enten helt eller delvis enig i påstanden «*Jeg utsetter meg selv for risiko når jeg bruker internett*». Vi ser en signifikant endring i perioden fra 2015 til 2019. I 2015 sa 58 % seg helt eller delvis enig i dette, mens det i 2019 er 73 % som svarer det samme.

Befolkningen opplever det som mer risikofyllt å bruke internett nå enn tidligere.
Videre sier 63 % seg helt eller delvis enig i påstanden *«Jeg synes at jeg får tilstrekkelig informasjon om de truslene som finnes på internett.»* 30 % sier seg helt eller delvis uenig i denne påstanden, mens 7 % sier at de ikke vet. Siden 2015 er det færre som mener at de får tilstrekkelig informasjon om truslene på nett.



Figur 16:
Jeg utsetter meg selv for risiko når jeg bruker internett.



Figur 17:
Jeg synes jeg får tilstrekkelig informasjon om de truslene som finnes på nett.

61 % av de spurte sier at de er i stand til å vurdere hva som er trygt og utrygt på nett, mens 23 % sier at de ikke er det.

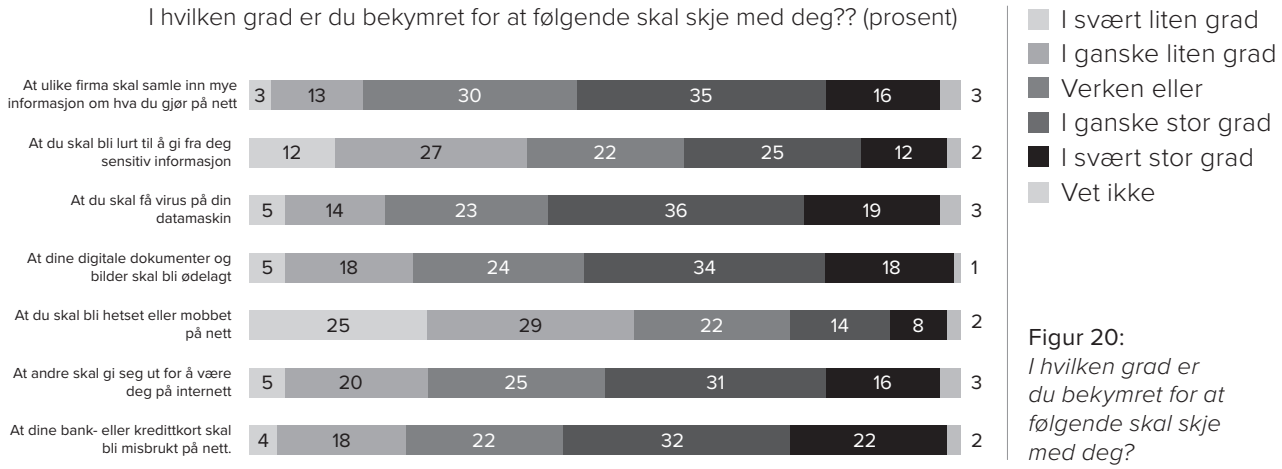
Det at nesten en tredjedel synes de ikke får nok informasjon om truslene ved bruk av internett, og nesten en fjerdedel mener de ikke er i stand til å vurdere hva som er trygt, forteller oss at det er et stort behov for å få ut informasjon om trusler på internett, og hvordan man kan motvirke truslene gjennom trygg bruk.

At nær 3 av 4 mener at det er like viktig å tenke på informasjonssikkerhet både hjemme og på jobb er også en indikator for risikooppfattelse i befolkningen. Vi observerer her at det er 15 % som mener det er viktigst hjemme, mens 6 % mener at det er viktigst på jobb eller på skolen

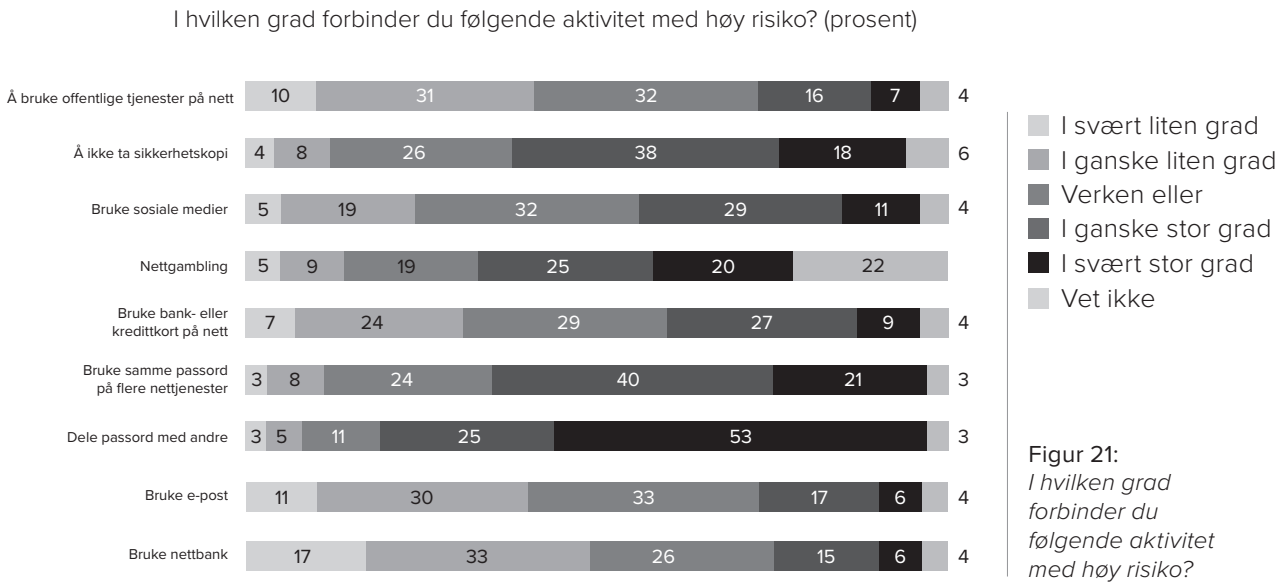
Vi spør også i hvilken grad den enkelte er bekymret for typiske trusler som rammer nordmenn på nett, og i hvilken grad befolkningen forbinder en del vanlige nett-aktiviteter med høy risiko.

Figur 18:
Føler du deg i stand til å vurdere hva som er trygt og utrygt på nett?

Figur 19:
Hvor synes du det er viktigst å tenke informasjons-sikkerhet?



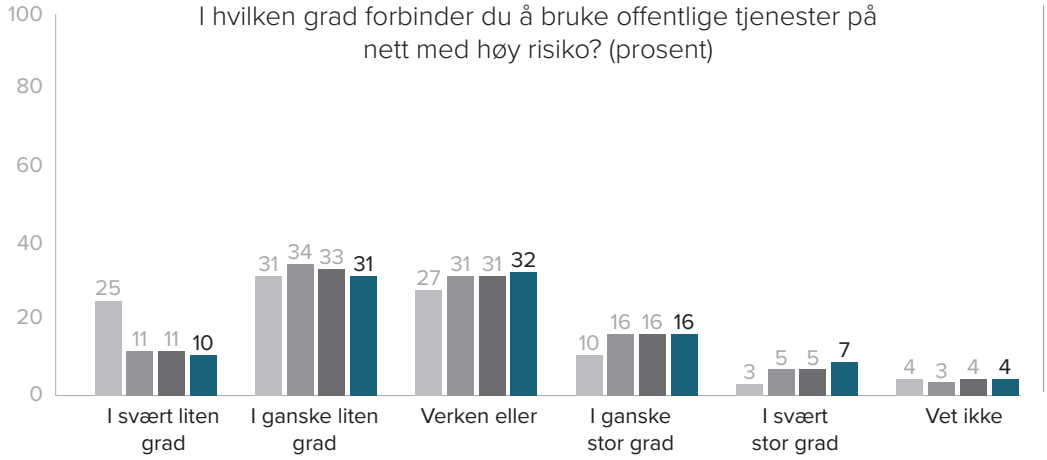
Figur 20:
I hvilken grad er du bekymret for at følgende skal skje med deg?



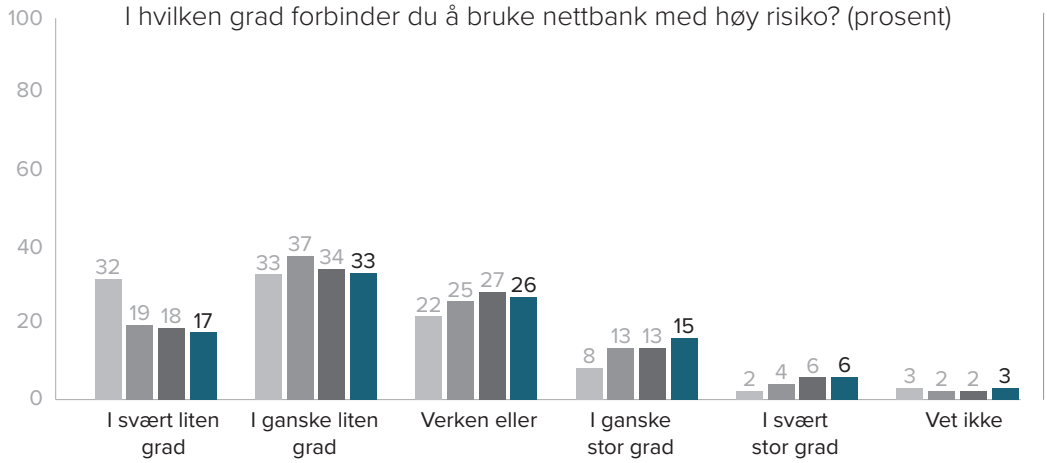
Figur 21:
I hvilken grad forbinder du følgende aktivitet med høy risiko?

Befolkningens risiko-oppfattelse for det å bruke offentlige tjenester på nett har endret seg siden vi undersøkte dette i 2015. Den gang svarte 13 % at de anså risikoen ved bruk av offentlige tjenester på nett å være enten ganske stor eller svært stor. Nå svarer 23 % det samme. Vi observerer med andre ord at frykten for dette øker i befolkningen.

Tilsvarende øker frykten for bruk av nettbank i den samme perioden. I 2015 svarte 10 % at de anså risikoen ved bruk av nettbank å være ganske stor eller svært stor, mens nå svarer 21 % det samme.



Figur 22:
I hvilken grad forbinder du å bruke offentlige tjenester på nett med høy risiko?



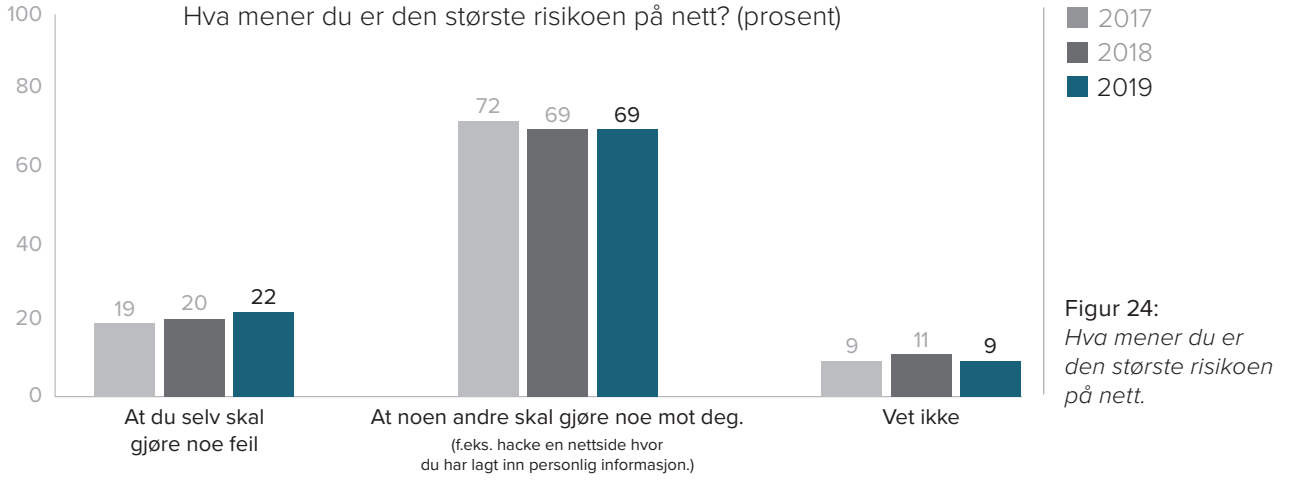
Figur 23:
I hvilken grad forbinder du å bruke nettbank med høy risiko?

Tillit er en forutsetning for at vi skal utnytte de muligheter som digitaliseringen gir. På samme tid kan frykt for digitale trusler redusere tilliten og føre til at den enkelte lar være å bruke digitale tjenester.

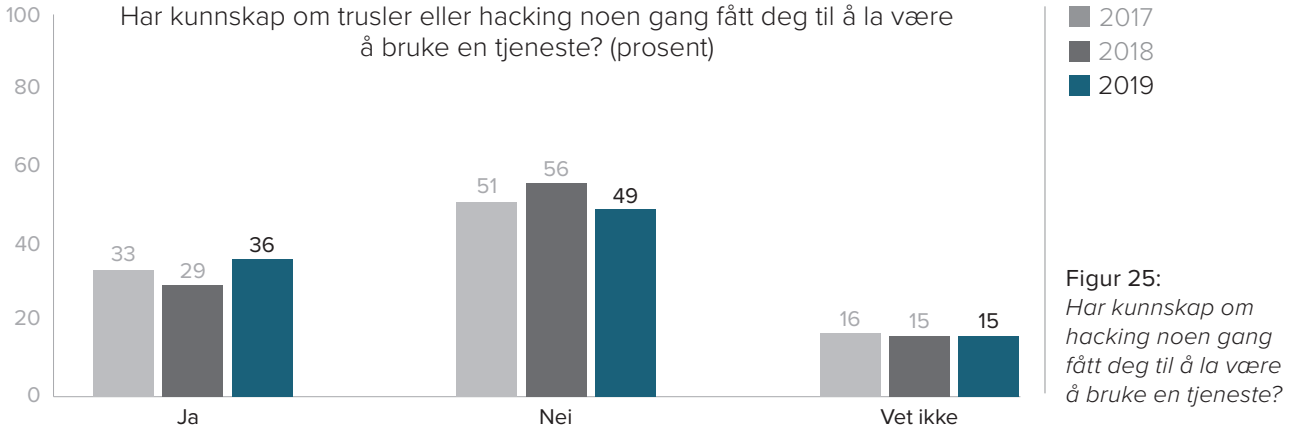
På spørsmålet «*Har kunnskap om trusler eller hacking noen gang fått deg til å la være å bruke en nettjeneste*», svarer 36 % Ja til dette. Dette er en signifikant økning fra 2018.

Frykt for trusler på nett kan bli en motvekt til digitaliseringsarbeidet og kan føre til en nedkjølingseffekt, altså at folk avstår fra å bruke nett-tjenester. Politiets bekjempelse av datakriminalitet og opplæring i trygg nettbruk er tiltak som trolig vil motvirke denne frykten.

Vi er også interessert i å vite om den enkelte ser på seg selv eller andre som den største risikoen på nett. Dette kan tolkes som et uttrykk for ens selvtillit når det gjelder digital sikkerhet. På spørsmålet *«Hva mener du er den største risikoen på nett?»* sier 22 % at de frykter at de selv skal gjøre noe feil, mens 69 % sier at de frykter at noen andre skal gjøre noe mot dem.

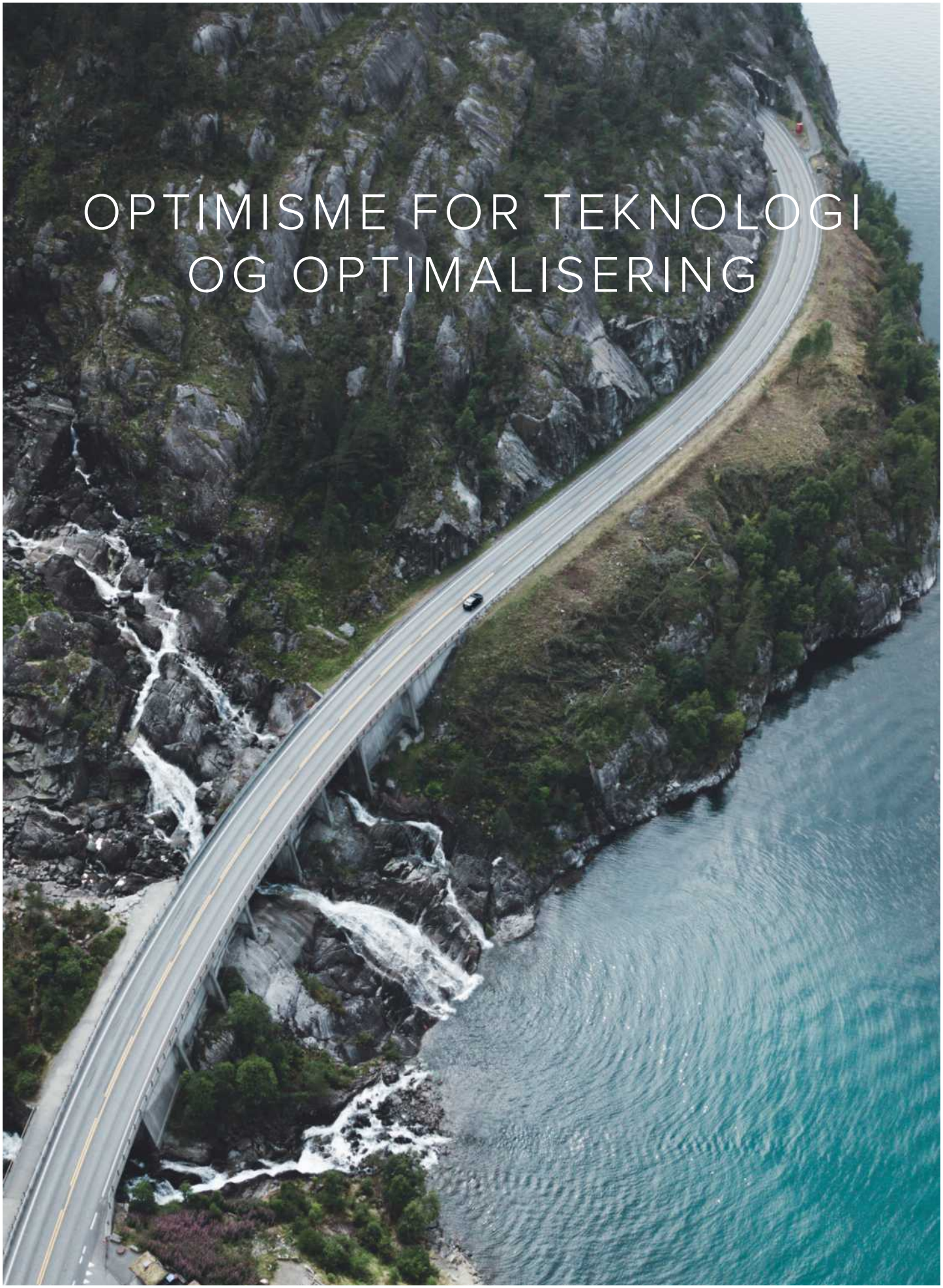


Figur 24:
Hva mener du er den største risikoen på nett.



Figur 25:
Har kunnskap om hacking noen gang fått deg til å la være å bruke en tjeneste?

OPTIMISME FOR TEKNOLOGI OG OPTIMALISERING

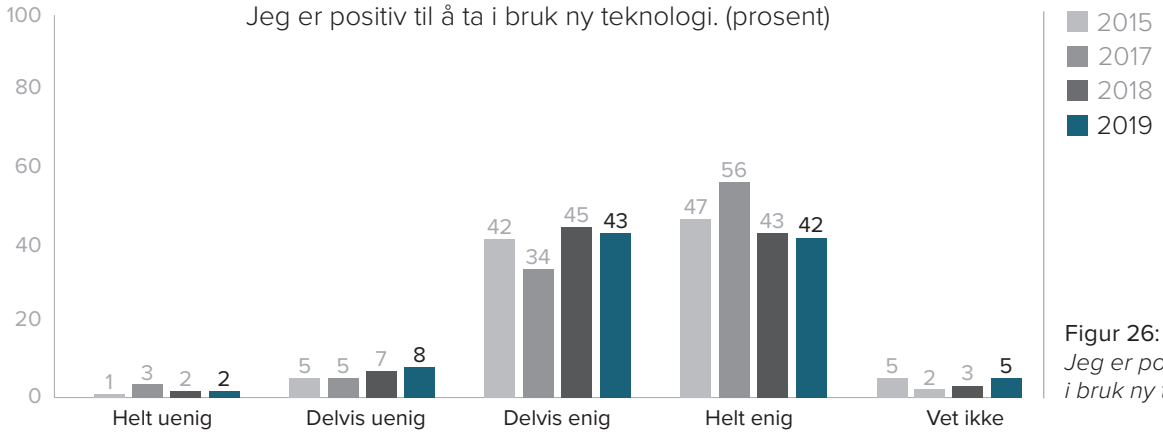


Digitaliseringen hjelper ikke bare bedrifter å bruke informasjonsteknologi og data på smartere måter, den sørger også for at den enkelte kan utnytte gevinstene av et digitalisert samfunn. I tillegg er digitaliseringen i samfunnet en stadig viktigere forutsetning for nasjonal økonomisk vekst og velferd. I forhold til digital sikkerhetskultur ønsker vi å se på befolkningens holdninger til denne utviklingen.

Med andre ord: Den enkeltes holdning til digitaliseringen påvirker måten man forholder seg til bruk av teknologi i samfunnet.

Folk i Norge er generelt svært positiv til å ta i bruk ny teknologi. 85 % sier at de er helt eller delvis enig i påstanden *«Jeg er positiv til å ta i bruk ny teknologi»*, mens 10 % er helt eller delvis uenig.

Å være positiv til noe betyr nødvendigvis ikke det samme som å være interessert i det. 43 % av befolkningen sier at de er ganske eller svært interessert i teknologi og IT, mens 28 % sier at de er ganske lite eller svært lite interessert i dette. Vi skal se nærmere på dette i et senere kapittel.



Figur 26:
Jeg er positiv til å ta i bruk ny teknologi.

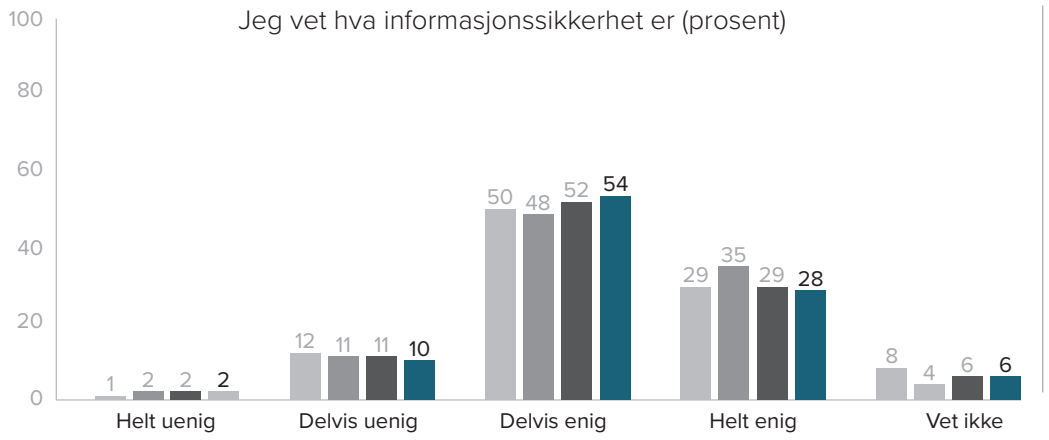

KOMPETANSE

ALT DEN ENKELTE FORETAR SEG, enten det er å ha kontakt med det offentlige, kommunisere med andre mennesker eller å dele feriebilder på sosiale medier, innebærer et element av å forholde seg til IKT og digitale tjenester. Dette betyr at alle nordmenn må ha et sett med grunnleggende digitale ferdigheter. Spørsmålet er: Hvor og hvordan får de disse ferdighetene? Det er et paradoks at myndigheter og bedrifter oppfordrer alle til å ta i bruk digitale tjenester, samtidig som slike ferdigheter bare i noen i grad inngår i skolens læreplaner eller i bedriftenes opplæringsprogrammer. Folk flest tvinges derfor til å lære disse ferdighetene på egenhånd og på uformelle arenaer.

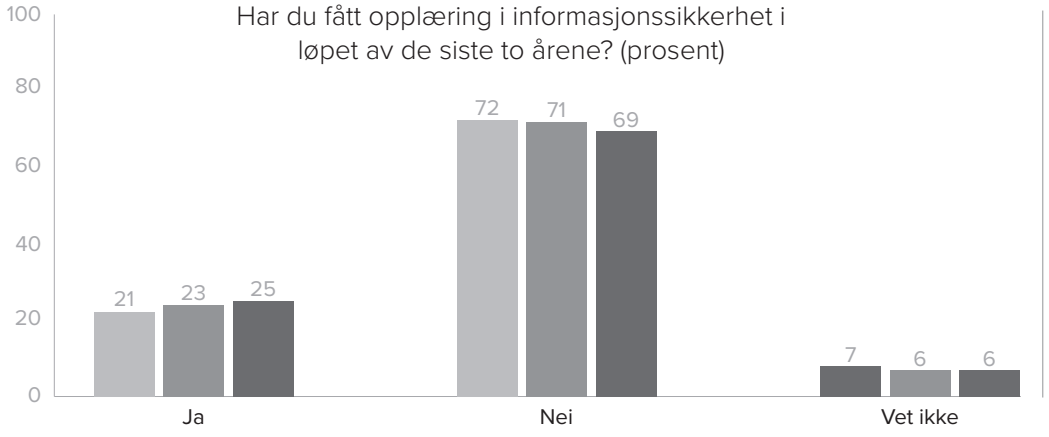
I alle kulturer lyttes noen mennesker mer til enn andre. Enten det er kjendiser eller eksperter på sine områder, får noen mer taletid og derfor en større mulighet til å påvirke oss andre. Disse menneskene har stor påvirkning på hvordan kulturen endres. De som beundres og lyttes til påvirker befolkningens verdier og holdninger. Gjennom dette påvirker de hvordan den enkelte av oss forholder oss til andre mennesker og våre adferdsmønstre. Gjennom å fokusere på dette vil vi undersøke hvem de sterke røstene er når det kommer til læring av informasjonssikkerhet. Lærer ulike grupper i samfunnet av forskjellige typer mennesker?

Nordmenn er generelt kunnskapsrike når det kommer til informasjonssikkerhet. De ser også på seg selv som relativt kunnskapsrike, og mener at de kan gjøre riktige vurderinger for sin sikkerhet på nett.

82 % er helt eller delvis enig i påstanden *«Jeg vet hva informasjonssikkerhet er»*. Imidlertid er det kun 25 % som sier at de har fått opplæring i informasjonssikkerhet i løpet av de to siste årene. 69 % sier de ikke har fått opplæring.



Figur 27: *Jeg vet hva informasjonssikkerhet er*



Figur 28: *Har du fått opplæring i informasjonssikkerhet de siste to årene?*

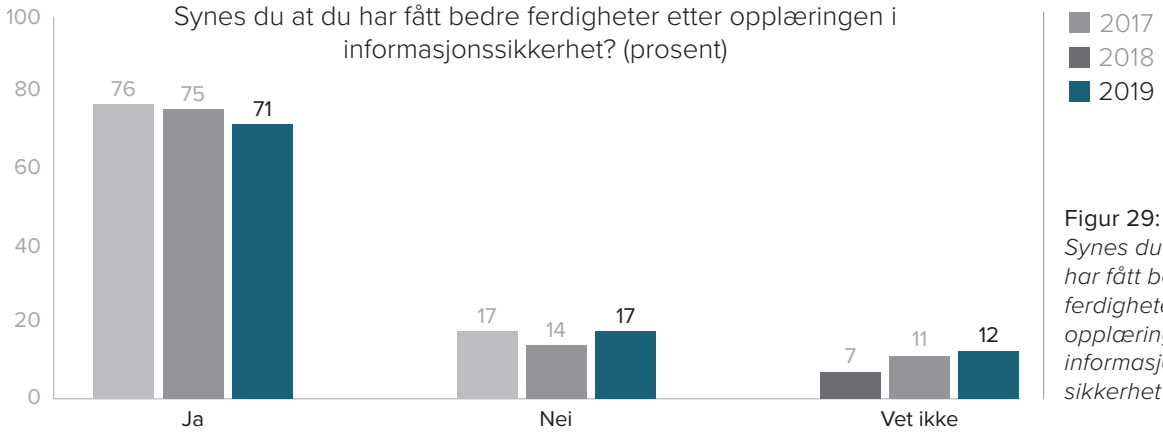
71 % mener at de har fått bedre ferdigheter etter slik opplæring, mens 17 % mener at de ikke har fått det.

Økt fokus på å nå ut med opplæring til en større del av befolkningen, kan derfor være et tiltak som kan være med på å bedre både forståelsen av digitale trusler, og som kan øke kunnskapen om trygg bruk av nettet.

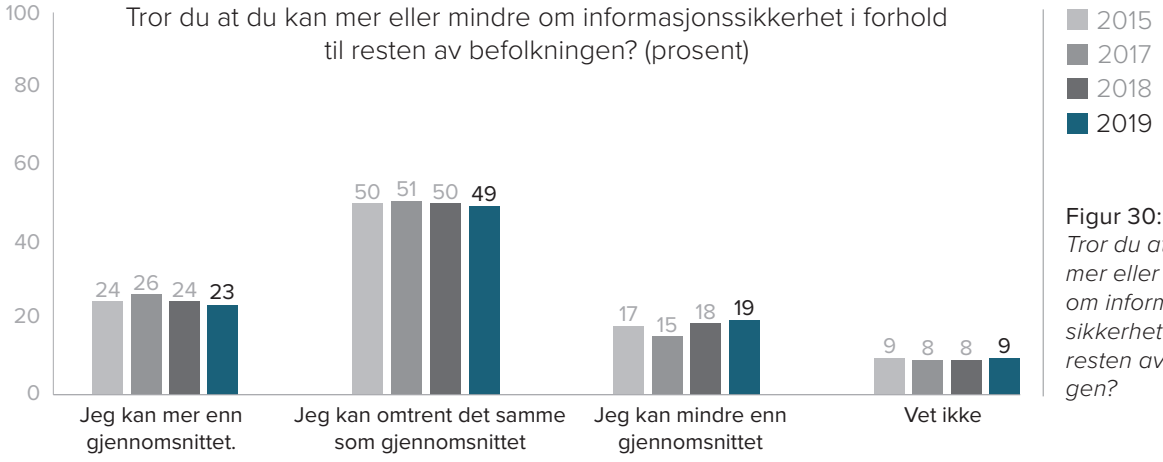
Generelt mener nordmenn at de kan like mye eller mer enn gjennomsnittet, når det kommer til informasjonssikkerhet. I befolkningen mener 49 % at de kan omtrent det samme som folk flest, mens 23 % mener at de kan mer en gjennomsnittet. 19 % mener at de kan mindre enn gjennomsnittet.

På spørsmålet *«Hvem lærer du mest om informasjonssikkerhet av?»* oppgir kun 17 % at de lærer av eksperter. Langt flere lærer av seg selv (37 %) eller av venner og kolleger (27 %).

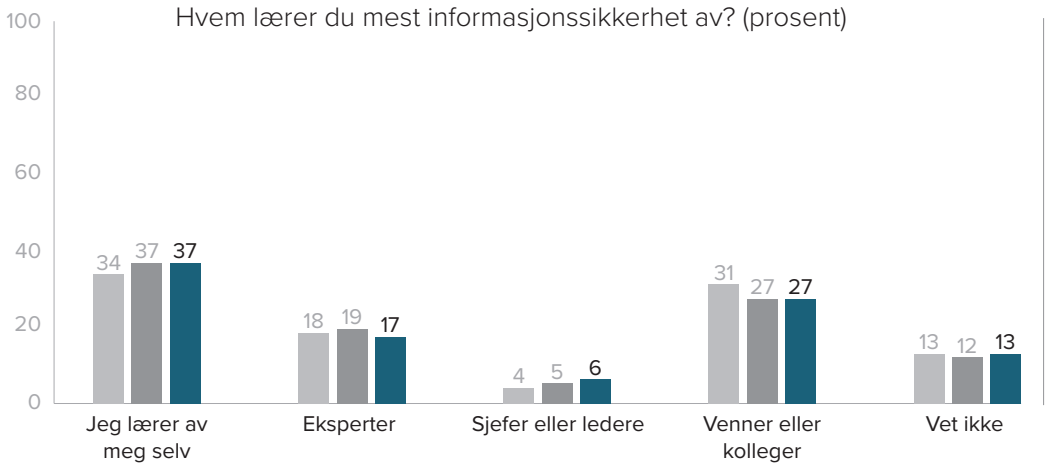
På spørsmålet *«Hvordan lærer du vanligvis om informasjonssikkerhet?»* oppgir 47 % at de hører om ting fra andre i en mer uformell situasjon, mens kun 17 % sier at de lærer på kurs eller utdanning. 24 % sier at de prøver og feiler selv.



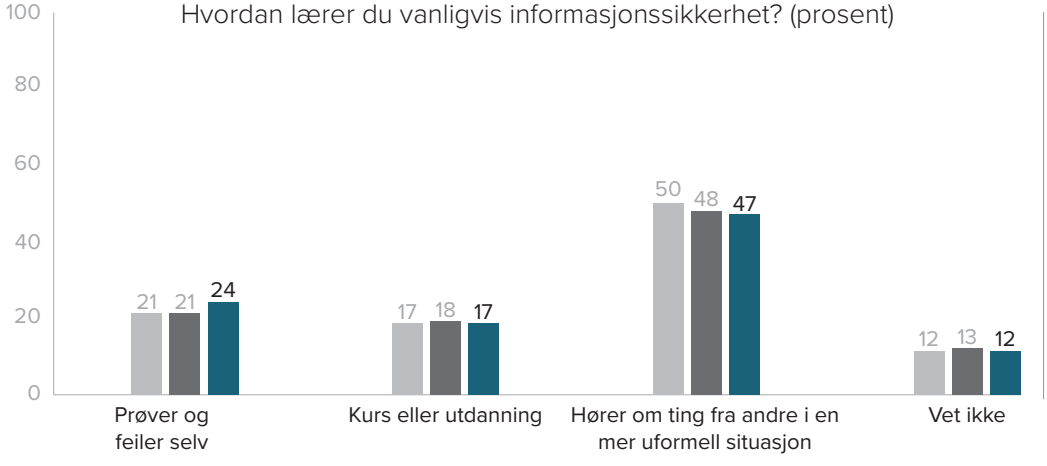
Figur 29:
Synes du at du har fått bedre ferdigheter etter opplæringen i informasjons-sikkerhet?



Figur 30:
Tror du at du kan mer eller mindre om informasjons-sikkerhet i forhold til resten av befolkningen?



Figur 31: *Hvem lærer du mest informasjons-sikkerhet av?*

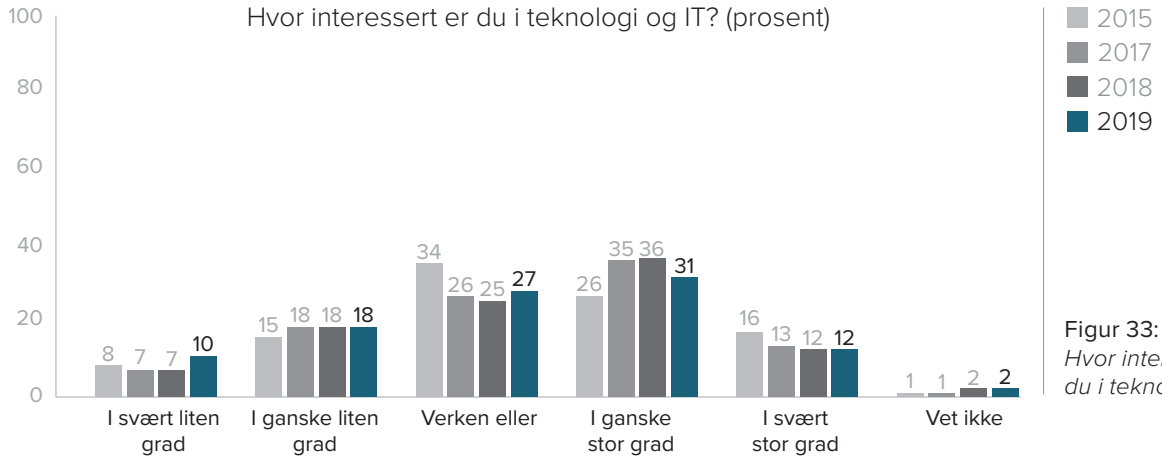


Figur 32: *Hvordan lærer du vanligvis informasjons-sikkerhet?*


INTERESSE FOR
TEKNOLOGI OG IT

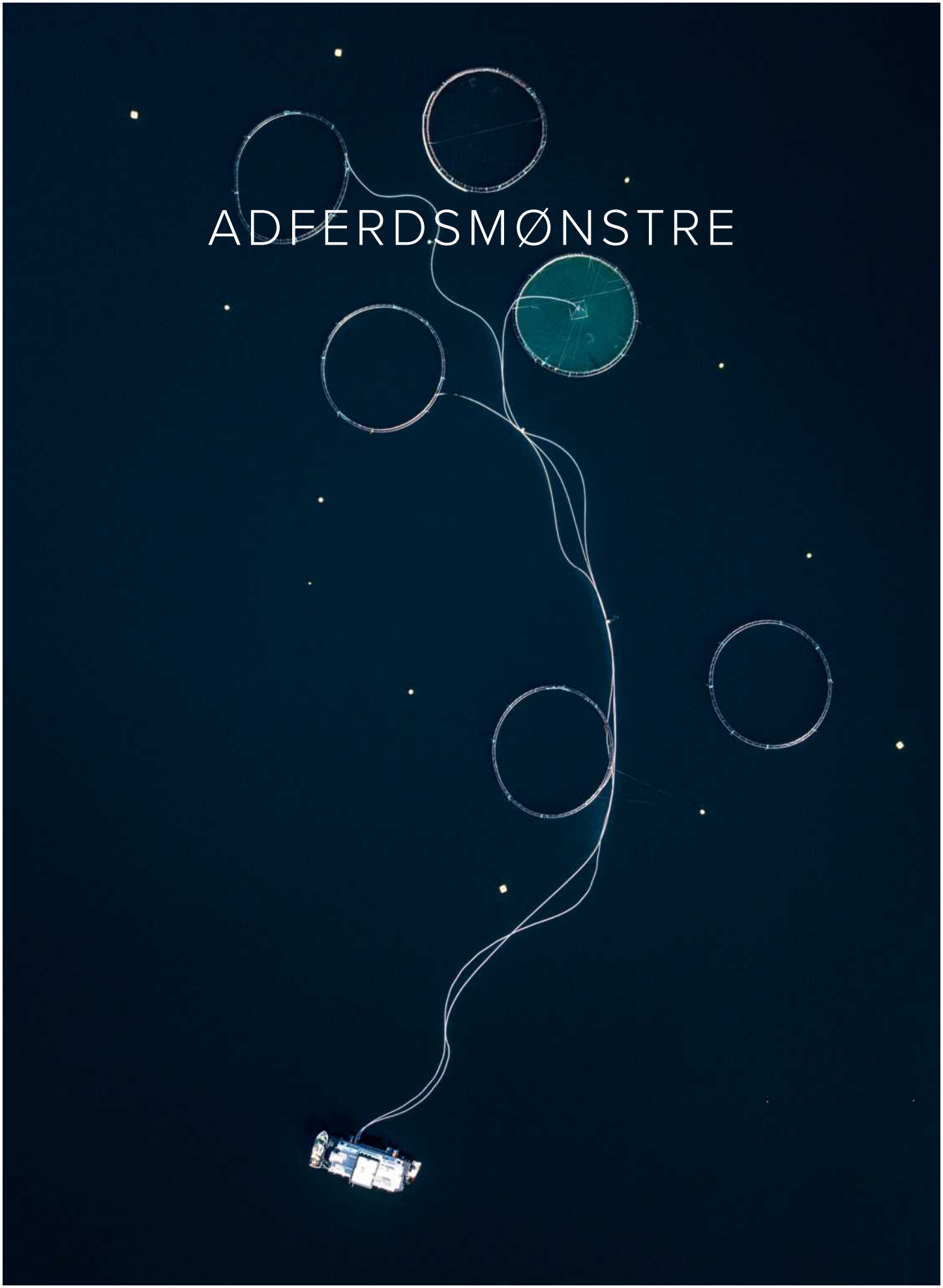
I vår hovedstudie fra 2016 slo vi fast at de som har interesse for teknologi og IT har en fordel i forhold til de som ikke har slike interesser. Interesser former våre holdninger, ferdigheter og kunnskaper. Interesse påvirker også hvem den enkelte assosierer seg med, og dermed hvem man lærer fra. Med interesse følger det bevissthet, nysgjerrighet og tid.

Dette er hjørnestener i all læring. Som en følge av dette mener vi at de som har interesse for teknologi og IT lærer raskere og "riktigere" enn de som ikke har det. Vi mener at interesse er en av kjerneområdene i digital sikkerhetskultur og at det derfor er viktig for deltakelsen i et digitalisert samfunn.



Figur 33:
Hvor interessert er du i teknologi og IT?

ADFERDSMØNSTRE



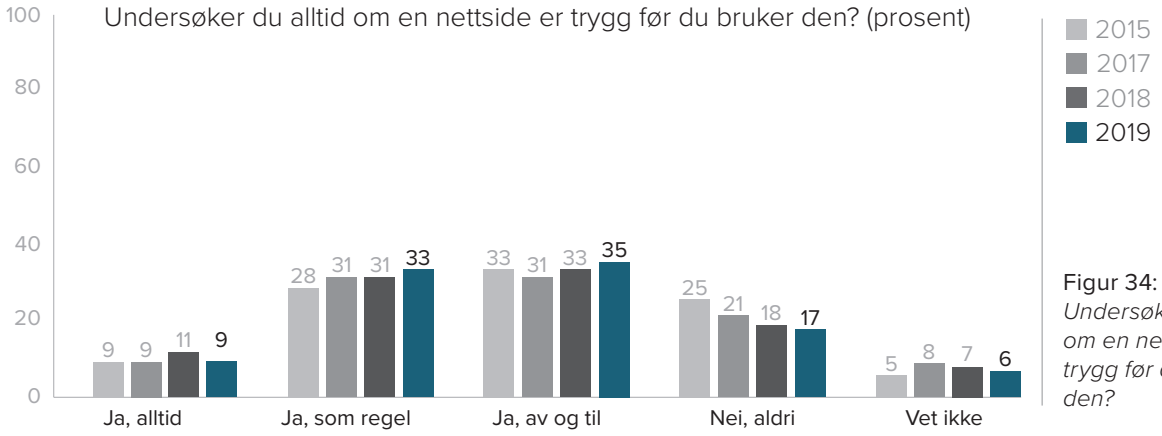
NÅR VI SER PÅ DIGITAL SIKKERHET er det visse typer adferd det oppfordres til, mens en advares mot andre typer adferd. Myndighetene, ledende selskaper og eksperter gir råd som i sum kan sees på som en normativ standard for hvordan innbyggerne og ansatte skal oppføre seg på nett. Når det er sagt, ekspertrådene og normene for "sikker adferd" har endret seg over tid. Dette er en naturlig konsekvens av den raske utviklingen i teknologien og hvordan teknologien tas i bruk. Dette betyr at det ikke er tilstrekkelig å få opplæring én gang. Opplæring må gjentas. Det du lærte for 10 år siden er ikke bare utdatert, det kan være direkte feil.

Når vi nå kartlegger digital sikkerhetskultur i befolkningen, så legger vi til grunn at det er en rekke ting vi oppfordrer alle å gjøre. Man bør ikke dele passordet sitt med andre, man bør ta sikkerhetskopi av viktige data og man bør sikkerhetsoppdatere programmene sine jevnlig. Dette er en del av dagens normative beskrivelse av hva sikker digital adferd er. Det oppfordres til dette for å redusere faren for datakriminalitet, for tap av informasjon og for at du ikke skal bli utsatt for manipulering og så videre.

17 % forteller at de aldri undersøker om en nettside er trygg før de bruker den. Det er en signifikant nedgang fra 2015.

NorSIS erfarer at sikker bruk av passord er krevende for mange. Tidligere var det vanlig å gi råd om passord som vi i dag tror er skadelig for sikkerheten. Kravene om at passordene skal være bygget opp av tilfeldige bokstaver, tall og spesialtegn og at de må skiftes med jevne mellomrom, fører til at mange bruker det samme passordet over alt. Passord som er vanskelige å huske for mennesker er paradoksalt nok ganske lette for en datamaskin å bryte. I dag gir vi råd om å bruke lange passord som er lette å huske (strofe fra en bok eller sang), gjerne med en tilpassing til det enkelte nettsted slik at en lettere kan velge forskjellige passord på de fleste nettsteder. Et annet, og kanskje enda viktigere råd er å skru på totrinns-verifisering der det er mulig. Da vil det ikke være mulig å logge seg inn på nettkontoen, selv om passordet har kommet på avveier.

For utfyllende råd om bruk av passord henviser vi til veiledninger på nettvett.no.



Figur 34:
Undersøker du alltid om en nettside er trygg før du bruker den?

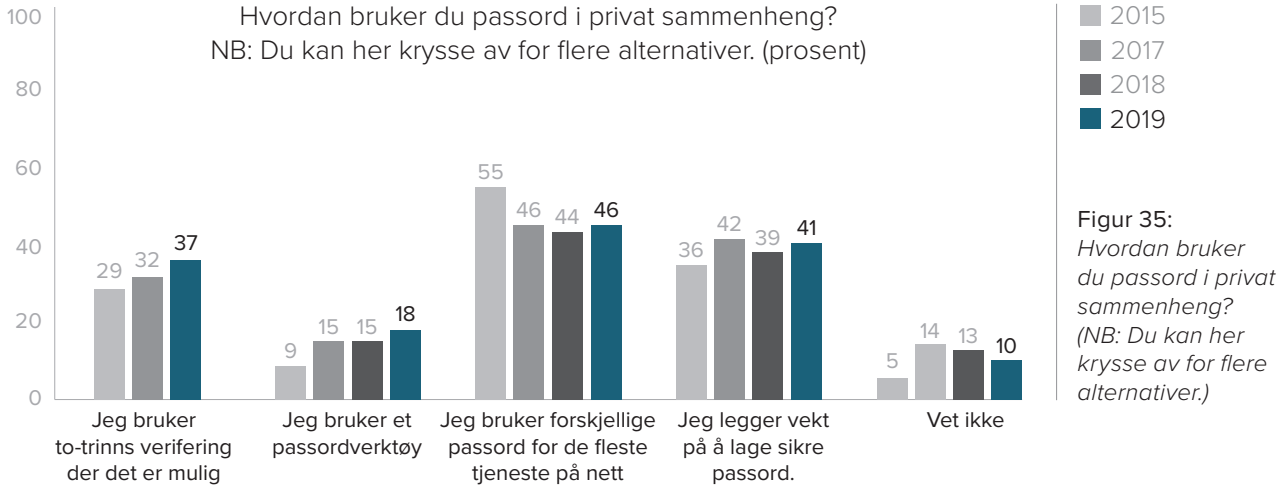
Det er nå 37 % av befolkningen som sier at de bruker totrinns-verifisering der det er mulig. Dette er en klar forbedring fra 2017.

Bruk av et passordverktøy for å håndtere ulike passord er også noe som anbefales, ikke minst fordi disse gir mulighet til å generere lange og tilfeldige passord som er vanskelig å bryte. Det er nå 18 % av befolkningen som sier at de bruker slike verktøy. Dette er en klar forbedring fra tidligere.

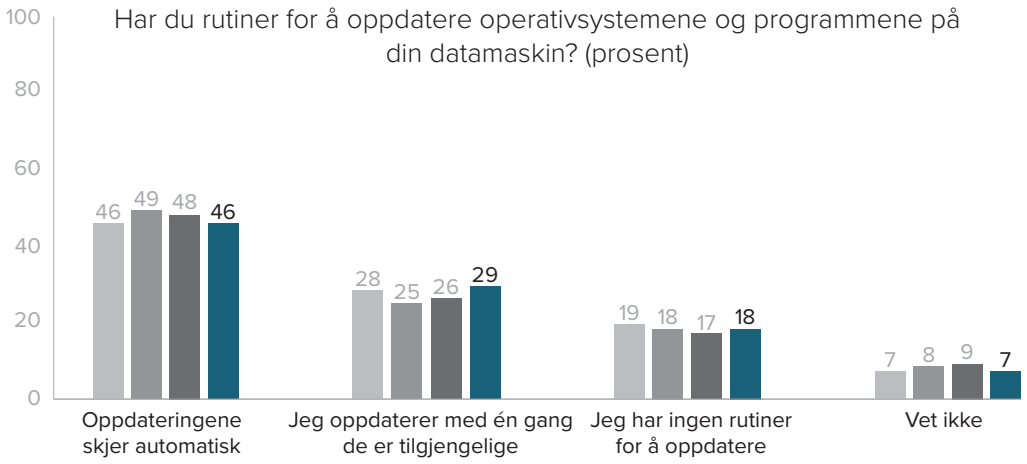
Det er ingen signifikante endringer i måten folk håndterer oppdatering av operativsystemer og programvare.

14 % sier at de aldri tar sikkerhetskopi av sine data og 14 % sier at de ikke vet om de gjør dette. De fleste som tar sikkerhetskopi (72 %) sier at de gjør dette sjeldnere en hver måned.

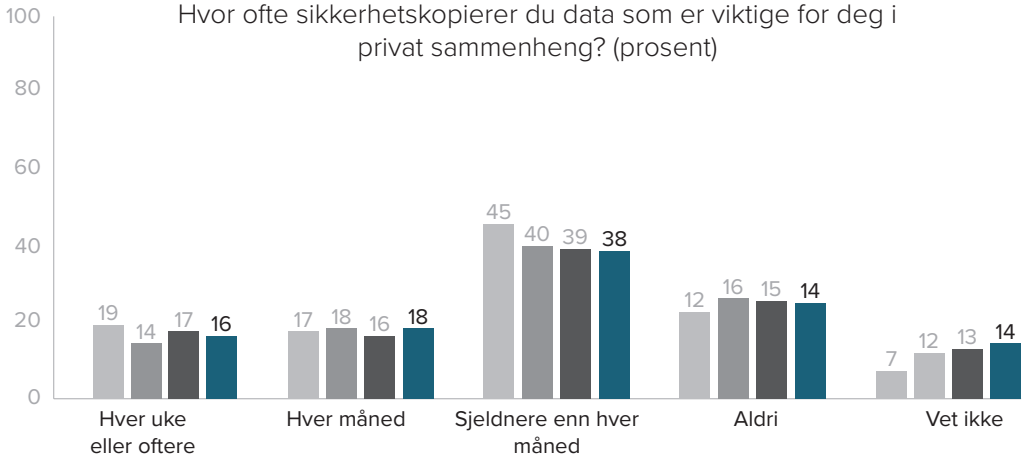
Nordmenn er generelt opptatt av personvern og å sørge for at personlig informasjon ikke faller i hendene på uvedkommende. Datamaskiner og mobiltelefoner inneholder stadig mer personlig informasjon, og vi er interessert i å vite hvor mange som selv vil sørge for å slette slik informasjon før slike enheter skal kastes eller selges. Vi ser ingen endringer i befolkningen omkring dette.



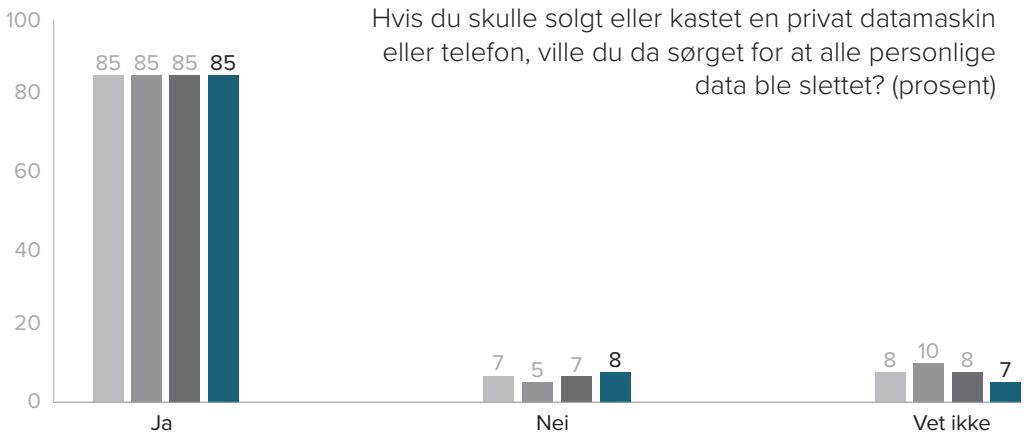
Figur 35:
Hvordan bruker du passord i privat sammenheng? (NB: Du kan her krysse av for flere alternativer.)



Figur 36:
Har du rutiner for å oppdatere operativ-systemene og programmene på din datamaskin? (prosent)

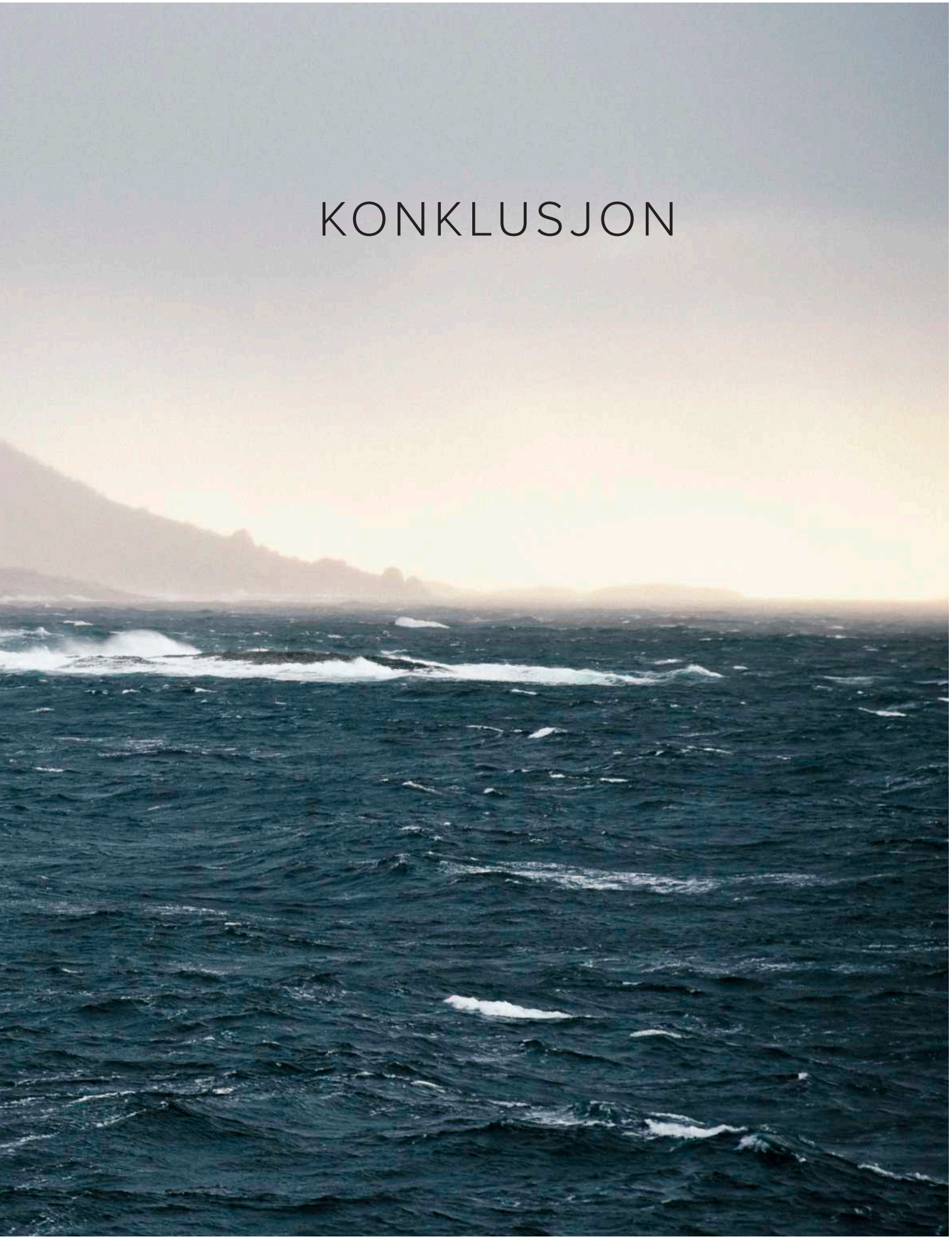


Figur 37:
Hvor ofte sikker-hetskopierer du data som er viktig for deg i privat sammen-heng? (prosent)



Figur 38:
Hvis du skulle solgt eller kastet en privat datamaskin eller telefon, ville du da sørget for at alle personlige data ble slettet? (prosent)

KONKLUSJON



også i årets rapport finner vi at nordmenn er dårlig rustet til å møte den digitale revolusjonen. Det er imidlertid tegn på at utviklingen går i positiv retning. Både NorSIS, NSM og andre aktører har hatt fokus på å opplyse om at bruk av totrinnsverifikasjon og passordmanagere. Dette er enkle tiltak som har stor effekt på sikkerheten. Vi ser nå en klar forbedring på begge disse tiltakene. Vi mener derfor at det nytter å opplyse om tiltak som alle kan ta i bruk.

På andre områder ser vi ingen endring. Dette gir grunn til bekymring fordi det er nødvendig at befolkningen blir tilført en oppdatert kunnskap om hvordan en skal beskytte seg mot kriminalitet og andre uønskede hendelser på nett.

Dette handler imidlertid ikke bare snakk om egenbeskyttelse. Digitale enheter i de tusen hjem kan også kan brukes til å angripe grunnleggende samfunnsfunksjoner eller til å begå nettkriminalitet i stor skala. Den enkeltes holdninger og praksis rundt digital sikkerhet kan derfor får store og direkte konsekvenser for samfunnet som helhet.

MASSEOVERVÅKING

Det er med stor interesse at vi følger med på hvordan større samfunnshendelser påvirker befolkningens holdninger til det digitale. Siden regjeringen har lagt frem et lovforslag om Etterretningstjenesten, der overvåking av datatrafikk inn og ut av Norge sto sentralt, var det interessant å se nærmere på hvorvidt dette har endret folks holdninger til styring og kontroll på nett. Undersøkelsen viser imidlertid at verken synet på overvåking av aktivitet på nett eller synet på hvorvidt det skal være mulig å være anonym har endret seg siden undersøkelsene vi gjorde før lovforslaget ble lagt frem.

Noe av forklaringen på dette kan være at relativt få sier at de har satt seg inn i hovedtrekkene i lovforslaget. Kun en av fem sier at de har gjort dette, mens hele 25 prosent sier at de ikke har hørt om lovforslaget. Lesere av fagpressen har neppe kunne unngå å få med seg debatten som fulgte, men det kan virke som om potensialet for å kommunisere dette bedre til befolkningen absolutt er til stede. NorSIS mener at dette er av svært stor betydning, nettopp fordi at en mulig holdningsendring som følge av en slik overvåking kan være at folk legger større bånd på seg hva gjelder bruk av digitale tjenester. Dette er en type nedkjølingseffekt som vi mener vil være svært negativt for det viktige digitaliseringsarbeidet som pågår.

ØKENDE FRYKT

Befolkningen fortsetter å oppfatte at både bruk av offentlige tjenester på nett og bruk av nettbank har høy risiko. Det er samtidig nå flere som sier at de har latt være å bruke digitale tjenester på grunn av frykt for hacking. Bildet er likevel nyansert. Når to tredjedeler mener at de er i stand til å avgjøre hva som er trygt å gjøre på nett. I tillegg sier en fjerdedel av de spurte sier at de har fått opplæring i digital sikkerhet i løpet av de to siste årene. Dette er en forsiktig økning i forhold til det de tidligere rapportene har vist.

NorSIS mener at dette likevel ikke er godt nok, fordi vi mener det er en sammenheng mellom opplæring i digital sikkerhet, synet på hvor risikabelt ting er på nett og hva den enkelte skal gjøre for at en selv og de rundt en skal være trygge på nett.

Vi satser derfor på å styrke våre opplæringstilbud, ved å utvide kursporteføljen på nettvett.no. Her publiserer vi gratis introduksjonskurs som målrettes mot ulike grupper i samfunnet.

Å redusere frykten for å bruke digitale tjenester er et mål i seg selv, og det er mange som deler ansvaret. Myndighetene må sørge for at det finnes tidsriktig informasjon om trusselbildet, og de må sammen med sikkerhetsbransjen og andre aktører som arbeider for digital sikkerhet sørge for at det finnes gode og effektive tiltak som både enkeltpersoner og bedrifter kan bruke.

HOLDNINGER OG NORMER

Innenfor vårt fagfelt er det vanlig å se at man snakker om å «bygge» eller «endre» sikkerhetskultur, presumptivt for å forbedre sikkerheten i virksomheter eller i samfunnet generelt. Noe av det som kjennetegner en kultur, er at menneskene som definerer seg som en del av den, deler et sett med verdier, holdninger og normer. Dette er grunnlaget for de handlingsmønstrene som folk i det fellesskapet har, og hvilke skikker de utvikler.

De som har tilhørt ulike grupper (som har sine egne verdier, holdninger og normer), eller som har arbeidet på ulike arbeidsplasser med sine egne bedriftskulturer, har sikkert sett at man forholder seg ulikt til de samme problemstillingene. Selv om reglene gjerne er de samme (man skal bære synlig adgangskort), oppfører man seg ulikt på forskjellige steder. Noen steder vil en kunne oppleve at enhver ansatt kan stoppe deg for å påpeke det dersom adgangskortet ikke synes, mens andre steder blir det ikke kommentert av noen. Noen grupper i samfunnet bryter bevisst reglene for digital sikkerhet, mens andre ikke gjør det. For noen grupper er det å dele et passord med andre helt utelukket, mens for andre er det helt vanlig.

Hvis vi ønsker å endre den digitale sikkerhetskulturen i en nasjon, samfunnsgruppe eller i en virksomhet, må en starte med å ha fokus på nettopp holdninger og normer. NorSIS tror ikke at svaret på alle utfordringene er å regulere dem gjennom lov eller forskrift. Da røykeloven ble innført endret den riktignok både folks adferd (det var ikke lenger lov å røyke inne), og etterhvert også folks holdninger til bruk av tobakk. Færre unge røyker i dag, enn før røykeloven ble innført. Selv om regulering antas å ha effekt på noen områder, mener vi likevel at regulering ikke bør være et hovedvirkemiddel når det kommer til digital sikkerhetskultur. Vi ønsker heller at det skal settes fokus på å formidle en tenkning rundt et digitalt fellesskap. Vi ønsker at den enkelte skal ta ansvar for sikkerheten til dem rundt seg, og for seg selv. Holdningen bør være at gjennom å sikre seg selv på nett, så blir også samfunnet sikrere. Normen bør være at man sier i fra og veileder dem som viser at de har en usikker adferd på nett. Dette mener vi vil stimulere til digital innovasjon og beskytte velferdsordningene og demokratiet mot digitale trusler.

I den nye nasjonale strategien for digital sikkerhet slås det fast at det i Norge skal være trygt å bruke digitale tjenester. Privatpersoner og virksomheter skal ha tillit til at den nasjonale sikkerheten og at den enkeltes velferd og demokratiske rettigheter blir ivaretatt i et digitalisert samfunn. Strategien legger vekt på at vi i fellesskap utvikler tiltak som kan styrke den digitale sikkerheten i samfunnet.

NorSIS imøteser derfor at flere aktører retter sitt fokus på de verdier, holdninger og normer som gjelder for befolkningens møte med det digitale. Vi trenger mer kunnskap om hvordan disse verdiene, holdningene og normene er, og ikke minst hvordan vi i fellesskap skal arbeide for å utvikle dem i en retning som styrker den digitale sikkerheten i samfunnet.

Teknologiveien 22
2815 Gjøvik
Org.nr. 995195003

Telefon: 40 00 58 99
www.norsis.no
post@norsis.no